N°19 - Avril/Juin 2019

LES DOSSIERS DU

Pirate

3,50 € seulement

100% FICHES PRATIQUES



DÉPANNER
BOOSTER
DÉSINFECTER
RÉPARER

89 PLANTAGES, BUGS & PROBLÈMES RÉSOLUS

Retrouvez un ordi tout neuf !

LE GUIDE 2019 ANTI-PLANTAGE



SAUVEGARDER
RESTAURER

VISIT…

LANZAROTE
Caliente.com



SOMMAIRE

EN PARTENARIAT AVEC

LES CAHIERS DU HACKER PIRATE [INFORMATIQUE]

MATÉRIEL

p10
Décortiquez et **TESTEZ** votre PC

p12
Testez tous les **COMPOSANTS**

p18
Maîtrisez la **TEMPÉRATURE** de votre PC

p20
REMPLACEZ les **COMPOSANTS** défaillants

p24
Mettez les **PILOTES** à jour

p28
MICROFICHES

SYSTÈME

p34
ENTRETENEZ Windows régulièrement

p38
Point de **RESTAURATION** : revenez en arrière !

p40
Désinstallez une mise à jour récalcitrante

p42
RÉPAREZ ou réinstallez Windows

p48
Retrouvez vos **CLÉS ET NUMÉROS** de licence

p50
Changez le **BOOT** depuis le **BIOS**

p52
MICROFICHES

DÉSINFECTER

p56
Les différents types de **MALWARES**

p59
AVIRA : le millésime 2019

p66
WINJA, le partenaire de votre antivirus

p71
MEDICAT : la **TROUSSE À OUTILS** universelle

p75
Protégez-vous des **RANSOMWARES** !

p78
MICROFICHES

SAUVEGARDER-RESTAURER

p82
SAUVEGARDER votre système et vos données

p88
Toutes nos pistes pour vos **SAUVEGARDES**

p92
Une **IMAGE MIROIR** de votre disque dur avec TestDisk

p96
RÉCUPÉREZ photos et fichiers perdus !

p98
SAUVEGARDEZ dans le **CLOUD**

LES DOSSIERS DU **Pirate**

N°19 - Avril – Juin 2019

Une publication du groupe ID Presse.
Impasse de l'Espéron - Villa Miramar
13960 Sausset Les Pins
E-mail : redaction@idpresse.com

Directeur de la publication :
David Côme
Saïtama : Benoît Bailleul
Genos : Shen Xue
Tatsumaki & Mumen Rider :
Stéphanie Compain & Sergueï Afanasiuk
Correctrice :
Marie-Line Bailleul

Imprimé en France par / Printed in France by :
Aubin Imprimeur
Chemin des Deux Croix
CS 70005
86240 Ligugé

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 2267-6295

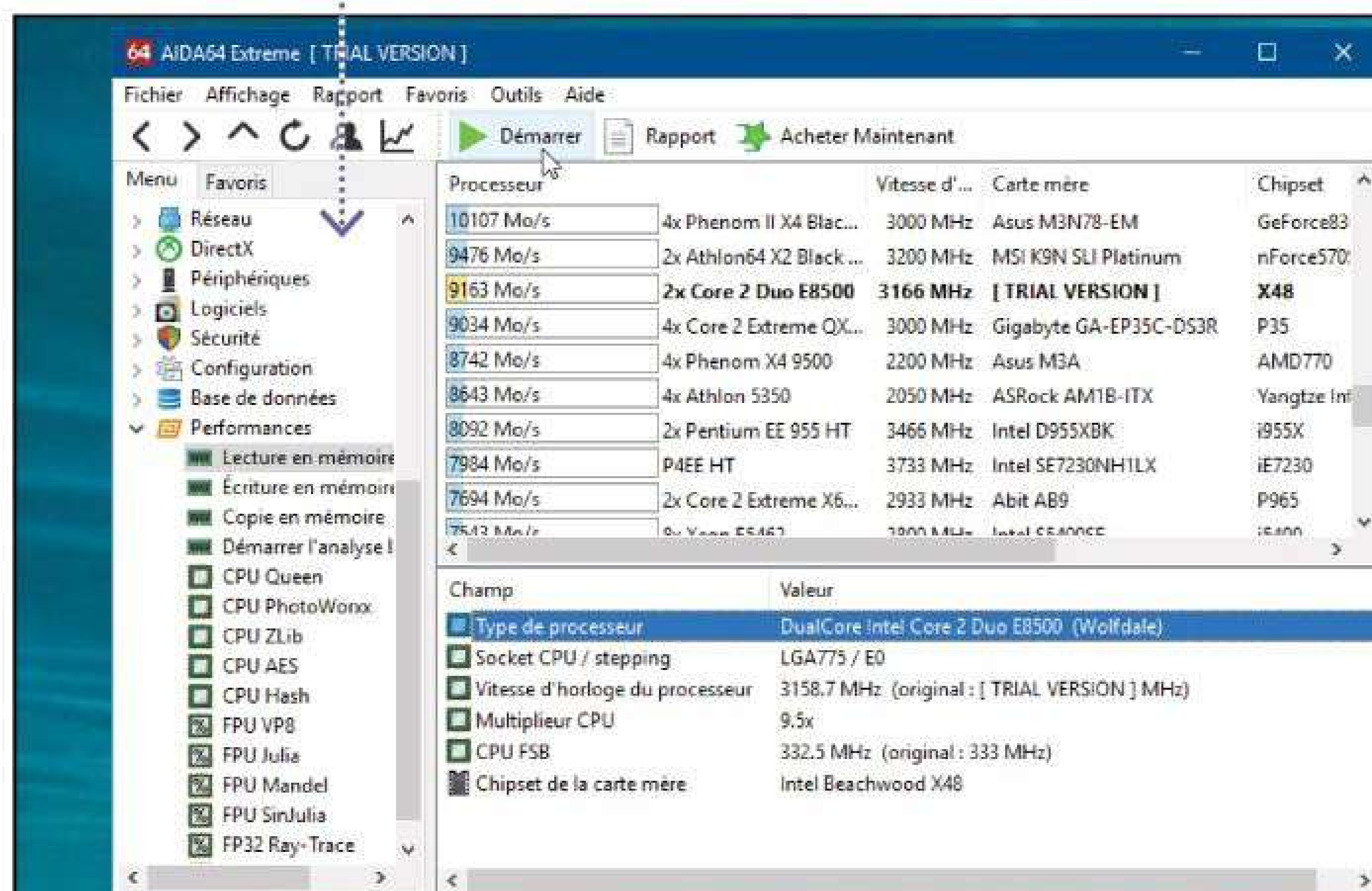
«Pirate» est édité par SARL ID Presse,
RCS : Aix-en-Provence 491 497 665
Parution : 4 numéros par an.

La reproduction, même partielle, des articles et illustrations parues dans «Pirate Informatique» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Sauf accord particulier, les manuscrits, photos et dessins adressés à la rédaction ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.

OUTILS ET SOLUTIONS

MATÉRIEL

Analysez les composants de votre PC afin d'identifier les problèmes.







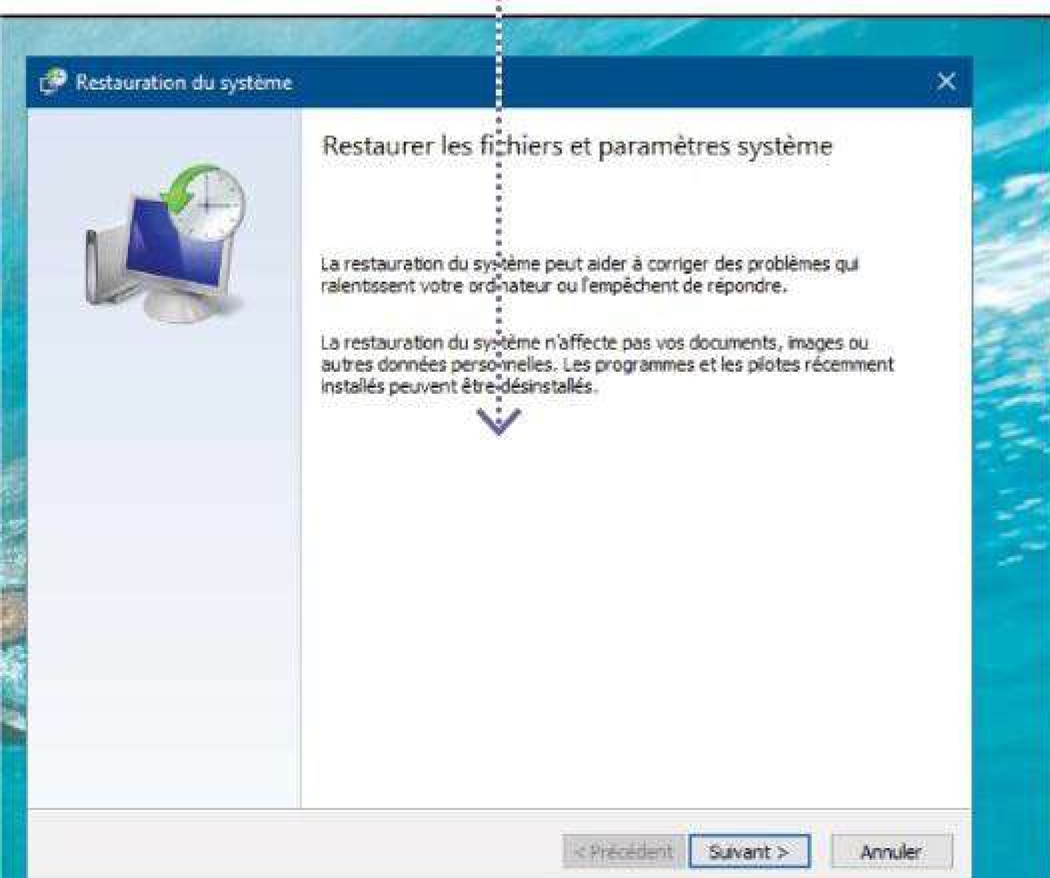


VIRUS

Complétez l'action de votre antivirus avec des outils spécialisés.

SYSTÈME

Windows intègre des fonctions pour réparer ses propres dysfonctionnements.



SAUVEGARDE

Prenez vos précautions pour pouvoir récupérer vos données en cas de souci.

Quelque chose ne tourne pas rond dans votre PC ? Avec un peu de méthode et les bons outils, vous devriez pouvoir résoudre le problème !

Votre PC peut vous faire vivre un véritable enfer lorsqu'il se met à ne plus tourner rond ! Messages incompréhensibles, blocages inexpliqués, fonctions qui ne fonctionnent plus… l'origine du problème n'est pas toujours facile à déterminer, et ses conséquences se traduisent au mieux par des énervements et du gaspillage de temps, au pire par des pertes de données et de documents importants.

MÉTHODE

Afin de vous éviter la crise de nerfs, nous vous proposons dans ce magazine des outils et des méthodes pour diagnostiquer le problème, déterminer s'il provient d'une panne matérielle, d'un logiciel inadapté, d'un dérèglement de Windows, ou d'une infection par un malware. Car en informatique, si les problèmes sont rarement compliqués sur le fond, le souci c'est qu'il y a souvent de très nombreuses causes possibles. Pour s'y retrouver, être efficace, il faut de la méthode.

SOLUTIONS

La cause du problème identifiée, reste à le résoudre. Changement d'un composant, réparation de Windows, éradication des virus, toute une panoplie de solutions sont évoquées dans les pages qui suivent. Reste éventuellement, une fois votre PC redevenu parfaitement fonctionnel, à récupérer les fichiers et données perdus dans l'aventure. Nous consacrons également tout un chapitre à cette question. En la matière, mieux vaut prévenir que guérir : eh oui, vous avez deviné, on va vous parler de sauvegardes !



PROCÉDEZ AVEC MÉTHODE !

Lorsqu'on rencontre un problème avec son PC, le plus dur est d'en déterminer la cause. Il faut pour cela un minimum de réflexion, et surtout de la méthode.



OBSERVER LES SYMPTÔMES



Que vous attaquiez vous-même la résolution du problème, demandiez de l'aide à un ami, ou cherchiez une solution via les forums Internet, il est essentiel au départ de bien décrire le ou les symptômes. Quand le problème est-il apparu pour la première fois ? Dans quelles circonstances survient-il ? Que se passe-t-il exactement ? Y-a-t-il des messages d'erreur (notez-les soigneusement) ?

ANALYSER LE PROBLÈME



Des messages d'erreurs évoquent spécifiquement des problèmes de mémoire ou de disque ? C'est sur ces composants qu'il faut se pencher. Si l'affichage connaît des perturbations, regardez du côté de la carte graphique. Des messages étranges et alarmants surgissent sans raison apparente, des publicités s'affichent à tout de bout de champ ? Vous êtes sans doute victime d'un virus. Un dysfonctionnement plus important, comme un blocage complet, est plus complexe à aborder : il peut s'agir d'une panne de matériel, ou d'un problème lié à Windows.

EFFECTUER DES TESTS

Procédez à des tests afin de valider ou d'éliminer les hypothèses. Commencez par les composants matériels s'ils peuvent être en cause, avant de vous pencher sur Windows : si les premiers ne fonctionnent pas, le second va forcément en pâtir ! Contre les infections virales, mobilisez non seulement votre antivirus, mais aussi d'autres outils spécialisés.



RÉSOUDRE LA PANNE

Si un composant de l'ordinateur est défaillant, il n'y a pas d'autre solution que le changer. Dans le cas des périphériques, il peut s'agir d'un problème de pilote, facile à résoudre. Lorsque Windows est en cause, si les tentatives de correction échouent (désinstallation d'une mise à jour, utilisation d'un point de restauration), il faut procéder à une réparation, voire une réinstallation complète du système. Pour une infection virale, les antivirus que nous vous conseillons devraient juguler l'infection, dans les cas les plus graves, une remise à zéro complète sera également à envisager.



RÉCUPÉRER SES DONNÉES

Les problèmes survenus sur votre ordinateur, ou de fausses manœuvres de votre part, peuvent provoquer des pertes de données plus ou moins importantes. Dans certains cas, une récupération a posteriori est possible, avec des utilitaires spécialisés. Mais la meilleure garantie, c'est de disposer d'une sauvegarde, à effectuer au plus vite si vous n'en disposez pas encore, et de toute urgence si des problèmes ont commencé à apparaître ! Suivez nos conseils.



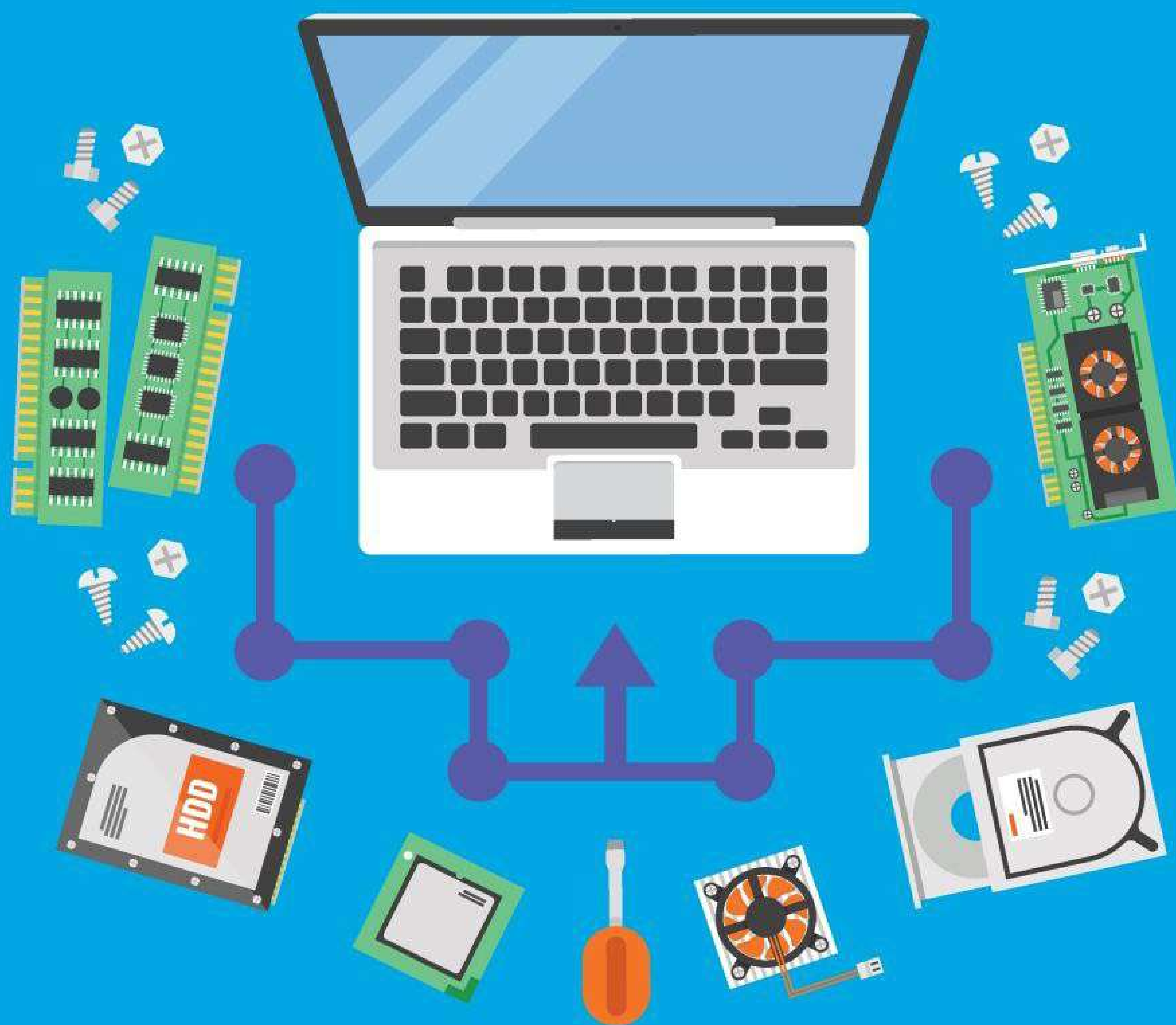
CHERCHEZ SUR INTERNET

Sur Internet, vous trouverez souvent quelqu'un qui a déjà eu votre problème et a demandé de l'aide. Choisissez bien vos mots clés, en y intégrant le cas échéant votre version de Windows, le nom du logiciel, ou le numéro d'erreur. Puis fouillez dans les résultats, en privilégiant les forums de discussion, et en cherchant la balise « résolu », indiquant qu'une solution a été trouvée.

L'INFORMATIQUE FACILE
POUR TOUS !



MATÉRIEL



p10
Décortiquez et **TESTEZ** votre PC

p12
Testez tous les **COMPOSANTS**

p18
Maîtrisez la **TEMPÉRATURE** de votre PC

p20
REMPLACEZ les **COMPOSANTS** défaillants

p24
Mettez les **PILOTES** à jour

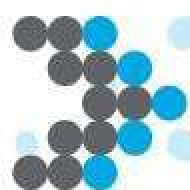
p28
MICROFICHES

DÉCORTIQUEZ ET TESTEZ VOTRE PC

Aïda 64 dresse la liste des composants internes de votre PC, et les pousse dans leurs derniers retranchements pour vérifier leur état de santé.



Dès son lancement, AIDA64 décortique votre PC : matériel, logiciels, pilotes, BIOS, Registre, il inventorie et analyse tout. Grâce à ses benchmarks intégrés, il va ensuite pouvoir jauger la puissance de votre configuration, et surtout réaliser un « stress test », consistant à faire tourner à fond l'ordinateur, le poussant dans ses derniers retranchements. Le but est de faire apparaître d'éventuelles faiblesses (surchauffe, voltage inadéquat, logiciel mal installé, etc.). Si un composant s'avère défaillant, l'identification précise de son type et de son modèle vous permettra de trouver facilement la pièce de remplacement. Notez que AIDA64 est payant (quelques dizaines d'euros), mais sa version d'essai de 30 jours permet de l'utiliser sans bourse délier pour un besoin ponctuel.



EN CAS DE PÉPIN, CONNAÎTRE SON PC DONNE UN NET AVANTAGE

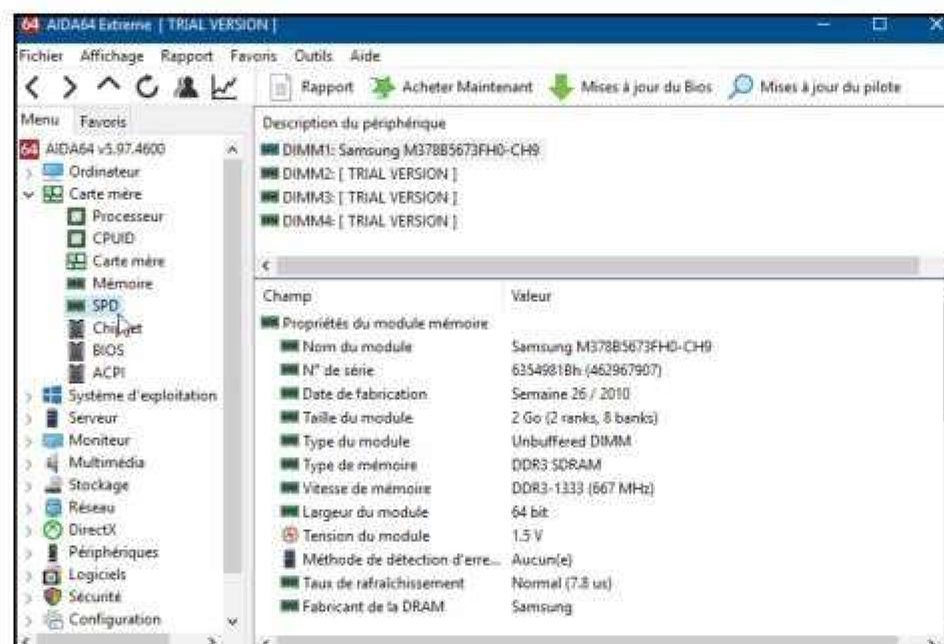
64 INFOS [AIDA64]

Où le trouver ? [www.aida64.com] Difficulté : ☠☠☠

TUTO

Downloads

	Version	Release Date	Size		
AIDA64 Extreme Trial version, self-installing EXE package	5.97.4600	Mar 28, 2018	48.97 MB	Buy now	Download
AIDA64 Extreme Trial version, portable ZIP package	5.97.4600	Mar 28, 2018	52.41 MB	Buy now	Download
AIDA64 Engineer Trial version, self-installing EXE package	5.97.4600	Mar 28, 2018	48.3 MB	Buy now	Download
AIDA64 Engineer Trial version, portable ZIP package	5.97.4600	Mar 28, 2018	51.74 MB	Buy now	Download
AIDA64 Business Trial version, portable ZIP package	5.97.4600	Mar 28, 2018	46.78 MB	Buy now	Download
AIDA64 Network Audit Trial version, portable ZIP package	5.97.4600	Mar 28, 2018	15.7 MB	Buy now	Download
AIDA64 for Android Download the app from Google Play			8.24 MB		Download
AIDA64 for iOS Download the app from App Store	1.17	Sept 25, 2017	24.1 MB		Download

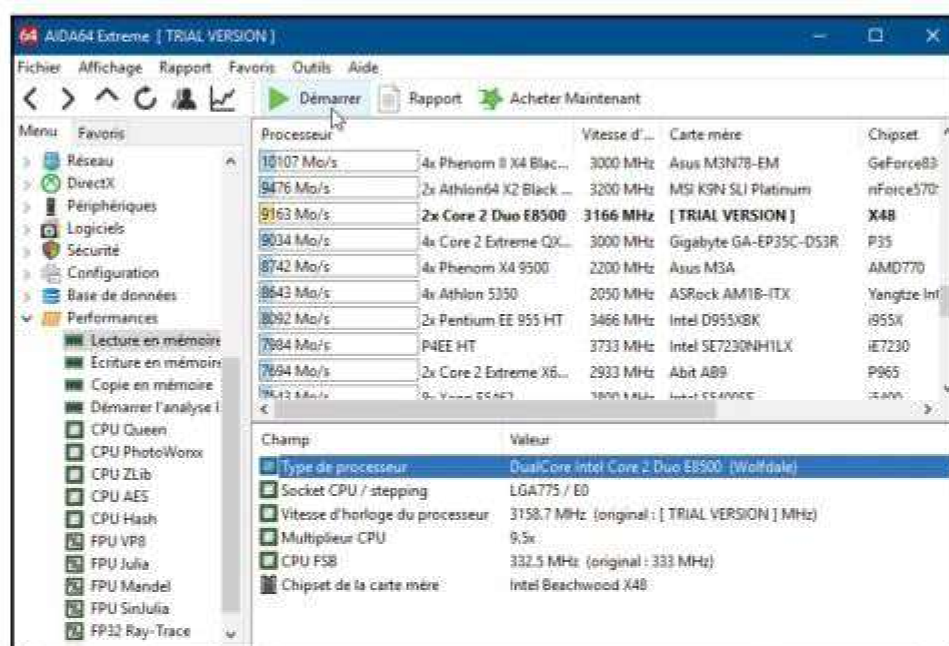


01 › TÉLÉCHARGER

Sur le site de l'éditeur, choisissez **Downloads**, en haut de la page, pour accéder au téléchargement. Optez pour l'édition **AIDA 64 Extreme**, en version installable classique (**EXE**), ou en version portable (**ZIP**) que vous pouvez mettre sur une clé USB : pratique si vous devez aller dépanner le PC d'un ami.

02 › LANCER LE LOGICIEL

Décompressez l'archive Zip téléchargée (clic droit, **Extraire tout**), puis double-cliquez sur **aida64.exe** pour lancer le logiciel. Explorez ensuite les diverses catégories et sous-catégories proposées dans la colonne de gauche pour tout savoir sur votre ordinateur.



03 › MESURER LES PERFORMANCES

Dans la catégorie **Performances**, vous trouvez différents outils pour tester les performances de votre processeur (cliquez sur **Démarrer**, en haut)). Pour chaque benchmark, vous avez des mesures effectuées sur d'autres composants que les vôtres pour comparer.

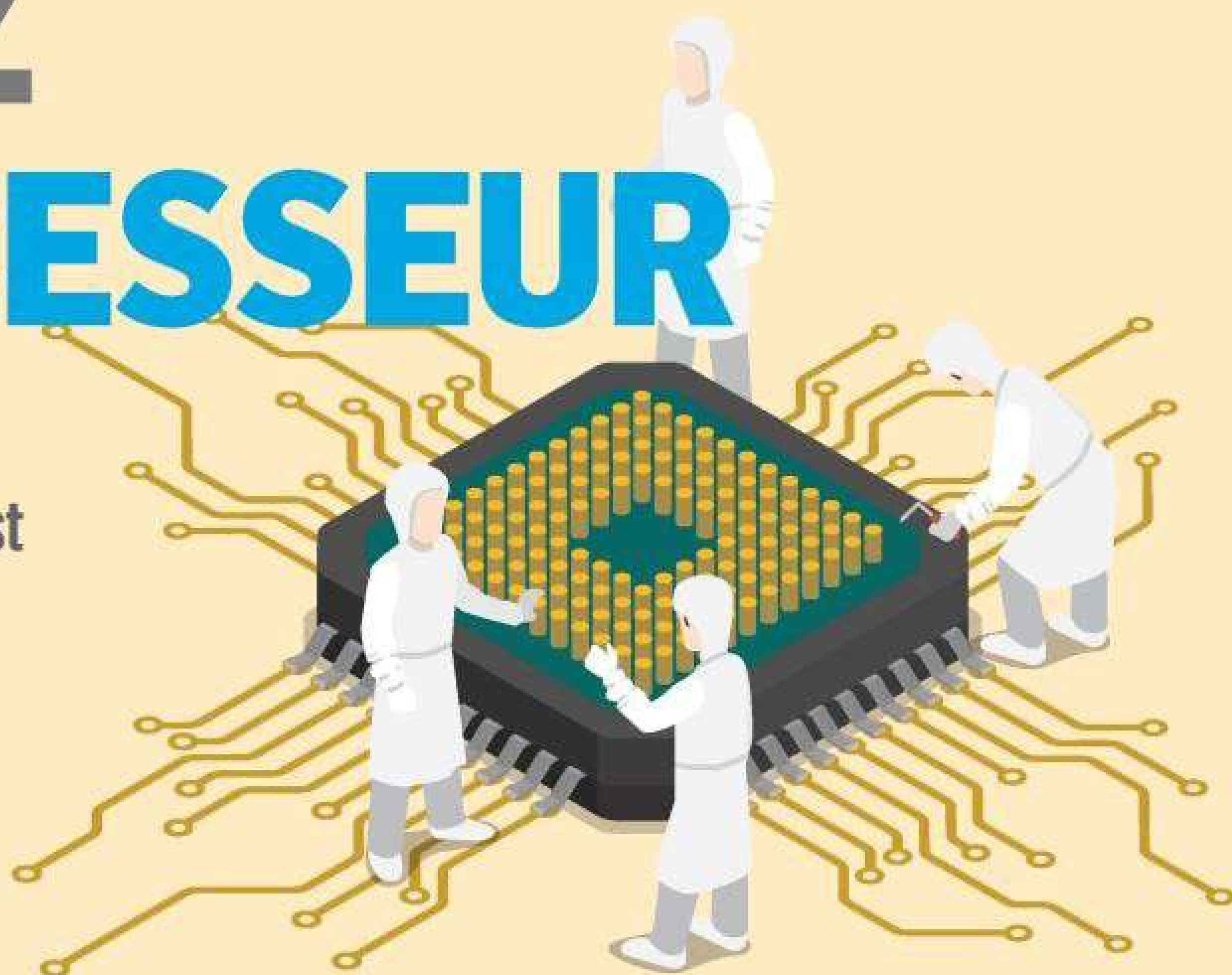


04 › VÉRIFIER LA STABILITÉ

Dans le menu **Outils**, choisissez **Test de stabilité système**. Ce « stress test » va faire fonctionner vos processeur, mémoire vive, carte graphique et disque dur à 100 % dans le but de vérifier le bon fonctionnement des ventilateurs, de contrôler la température, de mesurer le voltage ou les erreurs d'écriture sur l'espace de stockage.



TESTEZ LE PROCESSEUR

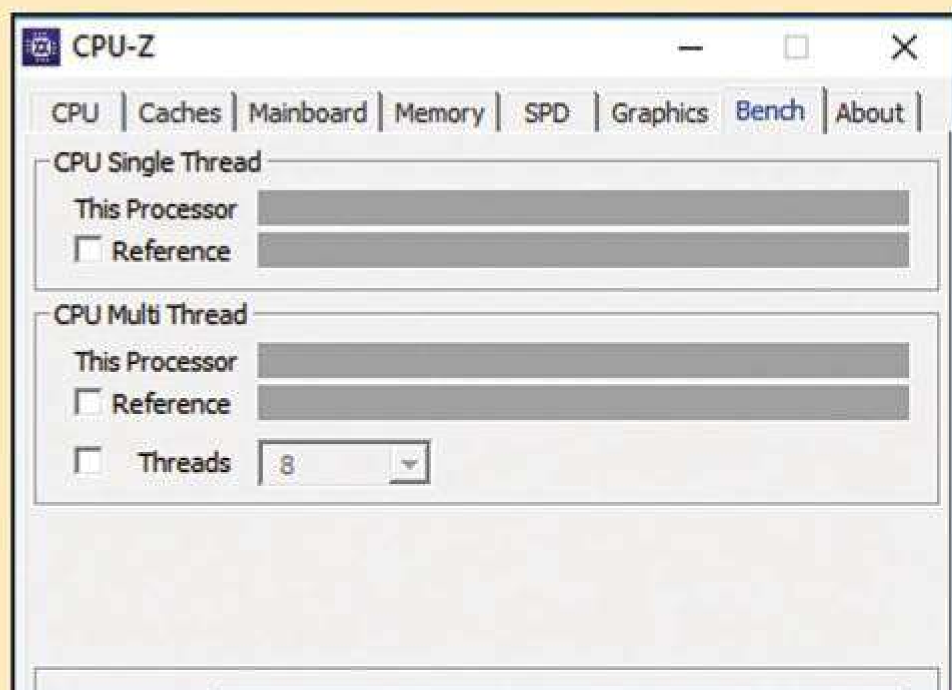


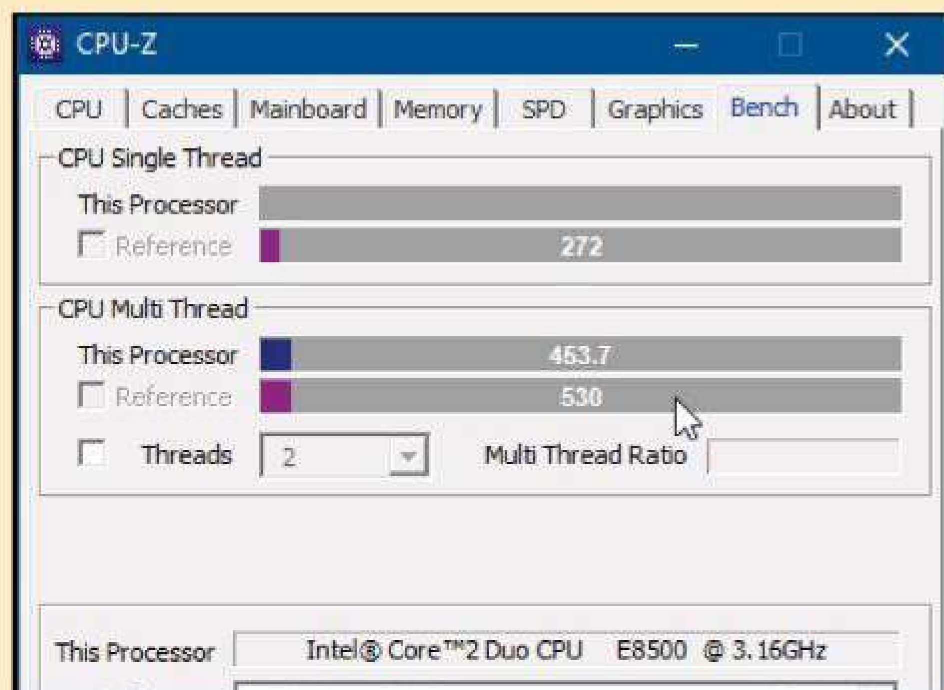
Le processeur est au cœur de l'ordinateur, et sa défaillance est susceptible d'entraîner un blocage de votre PC. Testez-le avec CPU-Z.



INFOS **[CPU-Z]**
Où le trouver ? [**www.cpuid.com**] Difficulté :

TUTO





01 › LANCER LE STRESS TEST

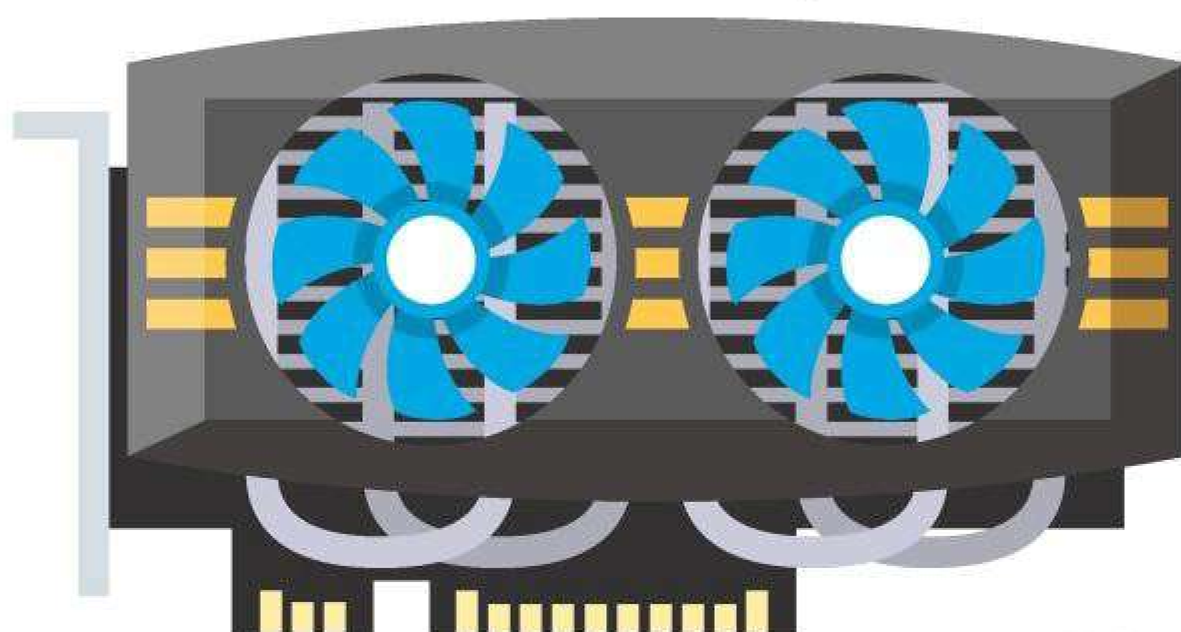
Rendez-vous sur l'onglet **Bench** de CPU-Z. Vous pouvez si vous le souhaitez sélectionner une **Reference** (tout en bas) pour comparer votre processeur à un autre, voire au fonctionnement normal de votre modèle s'il se trouve dans la liste. Cliquez sur **Stress CPU** pour démarrer. Tant que vous ne cliquez pas sur **Stop**, le processeur tourne au maximum de ses capacités.

02 › INTERPRÉTER LE RÉSULTAT

Il s'agit de voir si le PC « crashe » au bout d'un certain temps/pendant une certaine activité. Vous pouvez continuer à utiliser le PC, même s'il est très ralenti. S'il tient ainsi plusieurs heures, tout va bien. Si le PC s'éteint pendant le stress test, il y a sûrement un problème au niveau du processeur. Vérifiez notamment sa température.

VÉRIFIEZ LA CARTE GRAPHIQUE

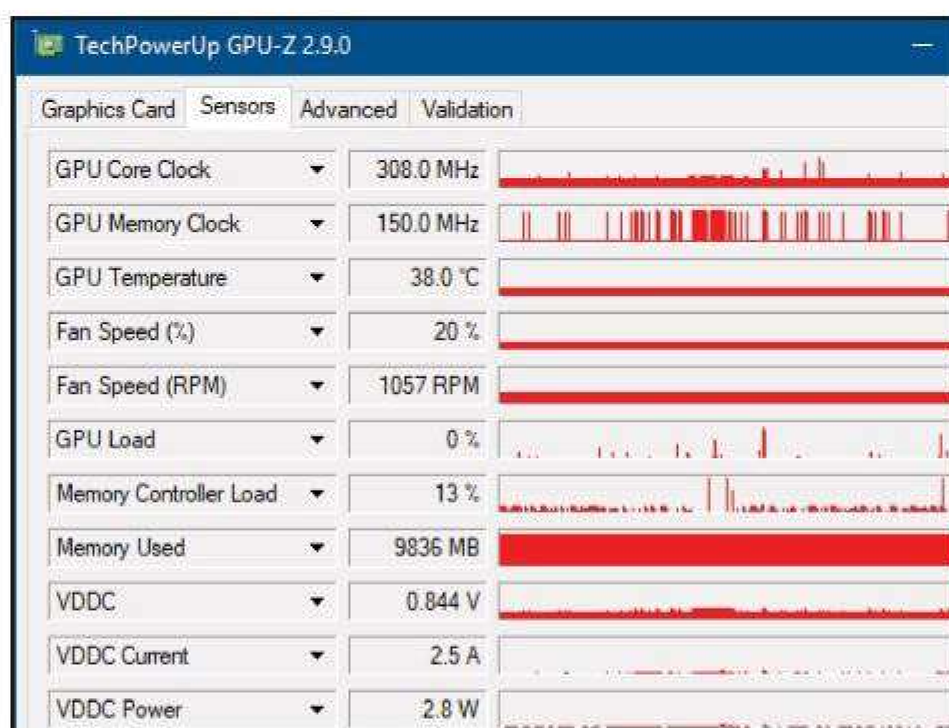
Vous rencontrez des problèmes d'affichage, des stries ou des zones vides apparaissent sur l'écran ? La carte graphique est peut-être en cause.





INFOS [GPU-Z]
Où le trouver ? [**www.techpowerup.com/gpuz**] Difficulté : ☠☠

TUTO



La Quintessence de Radeon™ Software
Apprenez-en plus sur l'expérience à couper le souffle proposée par Radeon Software.

Support AMD et logiciels Radeon (pilotes pou Radeon, FirePro, APU, processeurs, ordinateu de bureau, ordinateurs portables)

Récupérer les pilotes AMD
Procurez-vous les pilotes et les logiciels les plus récents pour vos produits AMD
TROUVER VOTRE PILOTE
Rechercher dans le support AMD
Rechercher...

01 › TESTER LA CARTE

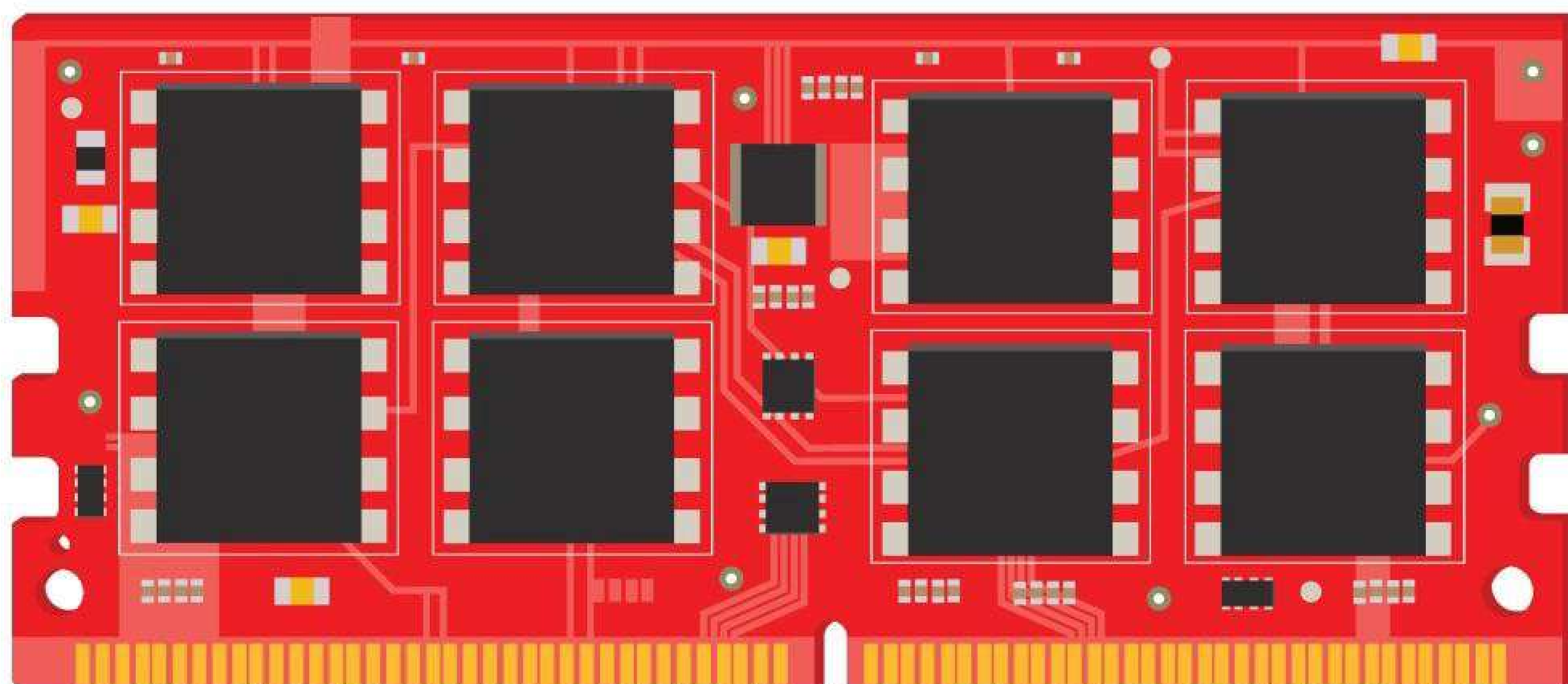
GPU-Z vous dit tout sur la carte graphique. Laissez le curseur de la souris sur un élément pour afficher une infobulle explicative. L'onglet **Sensors** permet d'afficher l'activité de la carte en temps réel. Regardez par exemple la ligne **Power** pour repérer une consommation anormale d'énergie, signe d'un dysfonctionnement.

02 › METTRE À JOUR LE PILOTE

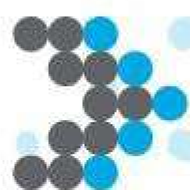
En cas de dysfonctionnements circonscrits à des logiciels (jeux en 3D par exemple), une mise à jour du pilote de la carte graphique peut résoudre les problèmes. Vous pouvez passer par un utilitaire comme DriversCloud, ou visiter directement le site du fabricant : **www.nvidia.fr**, ou **https://support.amd.com**, selon le cas.

ANALYSEZ LA MÉMOIRE VIVE

Plantages au chargement de Windows, redémarrages intempestifs, blocages ou messages inquiétants concernant la mémoire ? Il faut vérifier la RAM.



La RAM (ou mémoire vive) contient les éléments du système et les programmes qui sont en cours d'exécution. Si elle flanche, vous allez vous retrouver avec des erreurs aléatoires difficilement interprétables. Si votre Windows ne se charge pas correctement, plante à n'importe quel moment ou vous affiche des écrans bleus en pagaille cela peut venir de la RAM. De même si le système affiche des avertissements pour vous notifier que la mémoire est insuffisante ou des choses du genre **IRQL not less or equal** ou **Bad Pool Header**, cela peut s'expliquer par un problème de mémoire... Windows dispose d'une fonction permettant de vérifier l'intégrité des barrettes de RAM. Pas d'accès à Windows ? Les choses se compliquent...

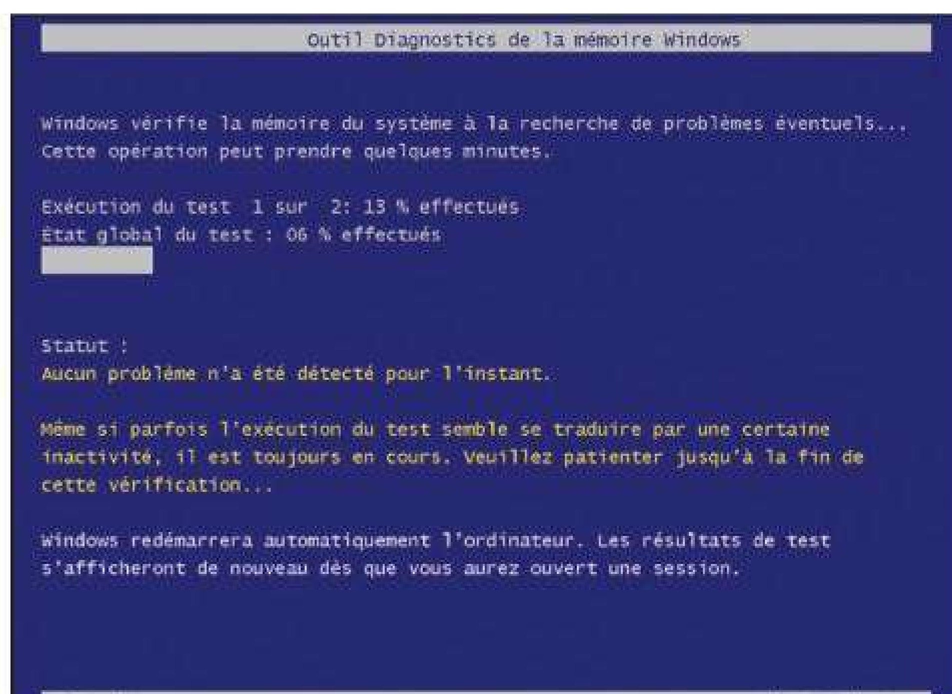


LE PROBLÈME AVEC LA RAM C'EST QU'UNE DÉFAILLANCE PEUT AVOIR PLUSIEURS SYMPTÔMES

Memtest86+

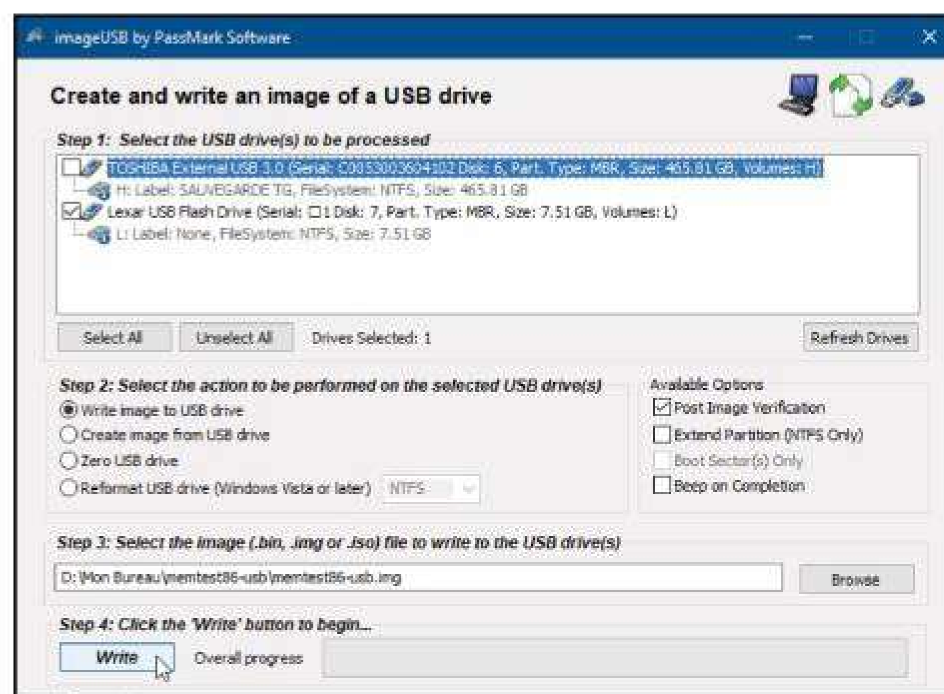
INFOS [MEMTEST86+]
Où le trouver ? [www.memtest.org] Difficulté : ☠☠☠

TUTO



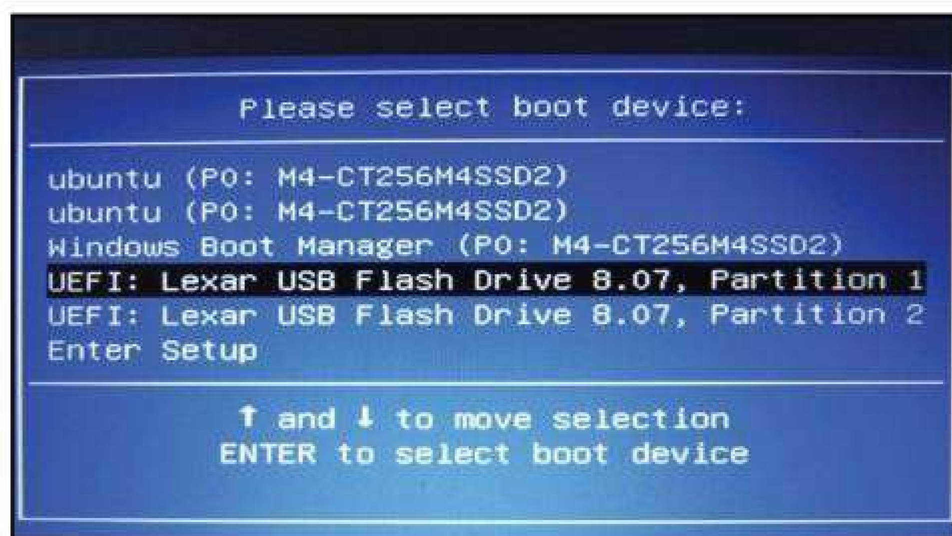
01 › ANALYSER LA RAM

Depuis sa version 7, Windows intègre un module permettant de vérifier l'intégrité des barrettes de RAM. C'est le premier outil à essayer. Tapez **mémoire** dans le champ de recherche et cliquez sur **Diagnostic de mémoire Windows**. Il faudra redémarrer puisque cet outil fonctionne avant même le chargement de l'OS.



02 › CRÉER UNE CLÉ USB BOOTABLE

Windows refuse de démarrer ? Il va falloir utiliser MemTest86, installé sur une clé USB bootable. Téléchargez **Image for creating bootable USB Drive**, dézippez le fichier et lancez-le après avoir introduit une clé USB vide dans votre PC (ou celui d'un ami puisque le vôtre est en panne !). Sélectionnez la lettre de votre clé et cliquez sur **Write**.



03 › DÉMARRER SUR LA CLÉ

Une fois que votre clé est prête, branchez-la sur votre ordinateur, allumez-le, et tapez immédiatement sur la touche permettant d'accéder au **Boot menu** (menu de démarrage), généralement la touche **Echap** (**Esc**) ou **F12**. Choisissez la clé USB comme dispositif de démarrage (**boot device**). Le test de mémoire est lancé automatiquement.



04 › TROUVER LA BARRETTE FAUTIVE

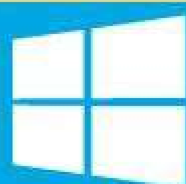
MemTest86 détecte les défaillances, mais pas la barrette de mémoire en cause : en cas d'erreur, il faut enlever une barrette de RAM et recommencer un diagnostic. Si vous n'avez plus d'erreur, c'est que la barrette que vous avez enlevée est défectueuse. Sinon, intervertissez les barrettes et relancez un test.



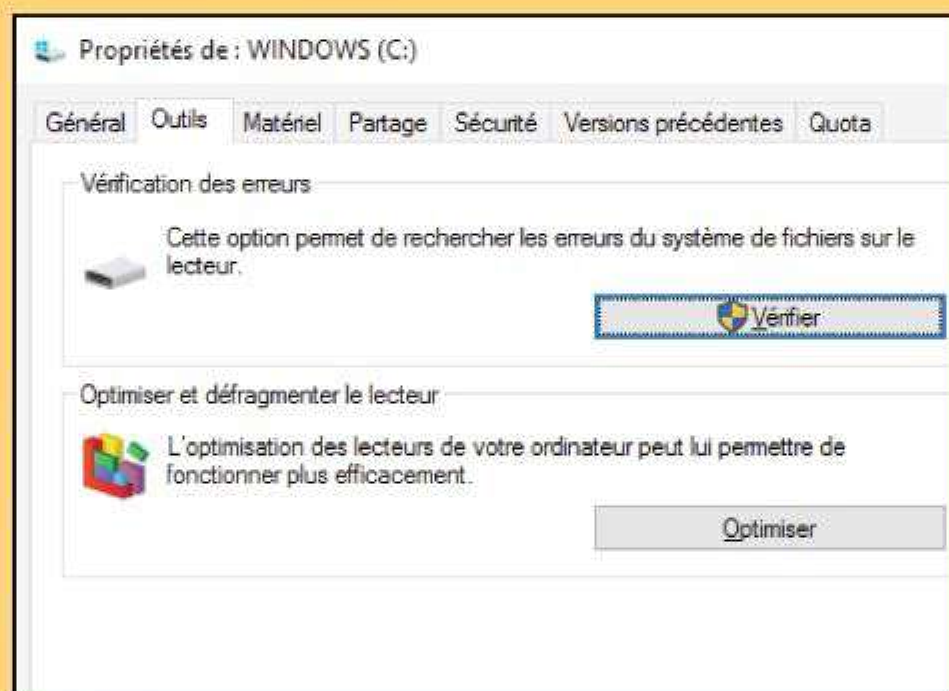
CONTRÔLEZ LE DISQUE DUR

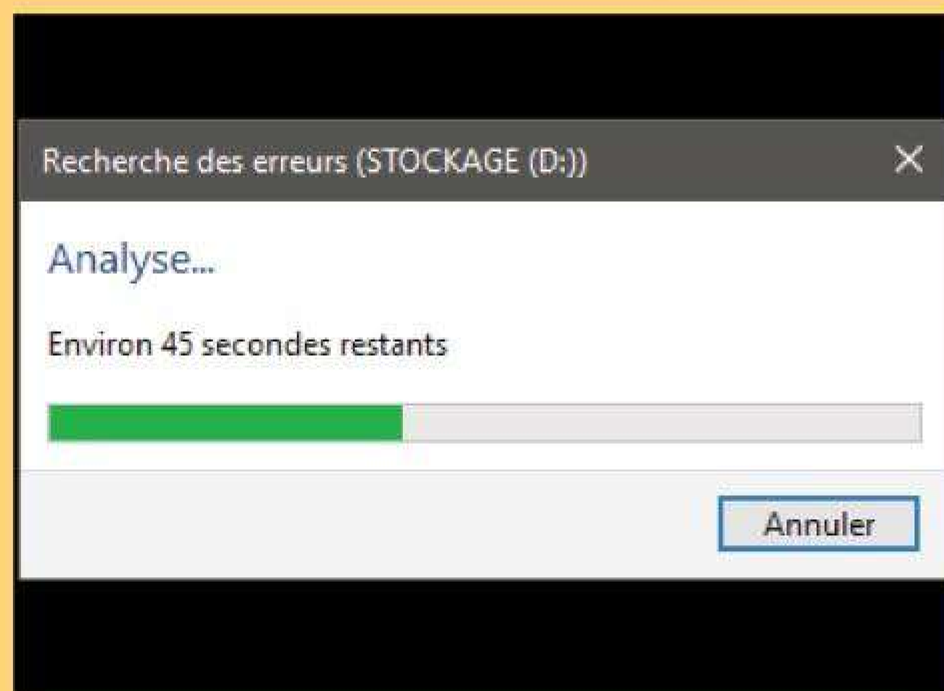


Activité anormale du disque dur, bruits inhabituels, lenteur insupportable de Windows ? Un test s'impose.



INFOS [WINDOWS] Difficulté : ☠ — TUTO





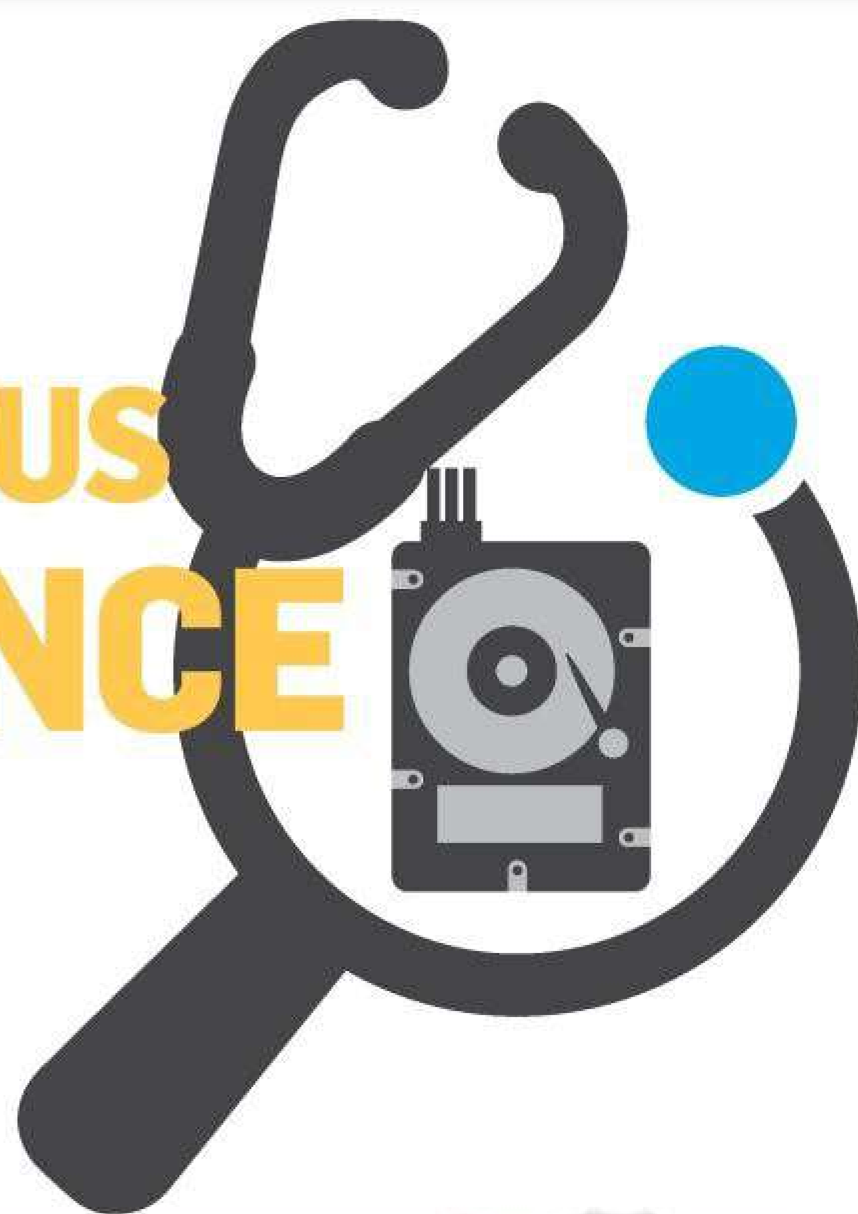
01 › LANCER LA VÉRIFICATION

Ouvrez l'Explorateur de fichiers, allez sur **Ce PC** ou **Ordinateur**, faites un clic droit sur le disque à vérifier et choisissez **Propriétés**. Trouvez alors l'onglet **Outils** et dans **Vérification des erreurs** cliquez sur **Vérifier**. Insistez si Windows vous affiche que ce n'est pas nécessaire.

02 › CORRIGER LES ERREURS

Lisez attentivement les messages qui s'affichent ensuite. Optez pour la réparation et la récupération à chaque fois : **Réparer automatiquement les erreurs de système de fichiers** et **Tenter une récupération des secteurs défectueux**.

METTEZ LE DISQUE SOUS SURVEILLANCE



Si les erreurs disque se multiplient, faites appel à un spécialiste. CrystalDiskInfo surveille vos disques en continu.



INFOS [CRYSTAL DISKINFO]
Où le trouver ? [**https://goo.gl/Suee**] Difficulté :

TUTO

Fichier Edition Fonctions Thèmes Disques Aide Language
Prudence
36 °C
C: E: G:

WDC WD2002FAEX-007BA0 2000,3 GB

Etat de Santé: Prudence
Température: 36 °C

Firmware: 05.01D05
Numéro de Série: WD-WMAWP0367643
Interface: Serial ATA
Mode de Transfert: SATA/600 | SATA/600
Lettre lecteur: C: E: G:
Standard: ATA8-ACS | ----
Caractéristiques: S.M.A.R.T., NCQ
Nbre d'allumage: 1485 x
Fonctionne depuis : 3884 heures

ID	Détail Caractéristique du ID	Actuel	Maxi	Seuil	Valeurs brutes
01	Taux Erreur en Lecture	199	188	51	0000000015D9
03	Temps moyen mise en rotation	253	253	21	0000000020F1
04	Décompte des cycles de mise en rotation	99	99	0	0000000005ED
05	Nombre de secteurs réalloués	200	200	140	000000000000
07	Taux d'erreurs d'accès des têtes	100	253	0	000000000000
09	Heures de Fonctionnement	95	95	0	000000000F2C
0A	Nombre d'essais de relancement de la r...	100	100	0	000000000000
0B	Nombre de recalibration	100	100	0	000000000000
0C	Nombre total de cycles marche/arrêt du ...	99	99	0	0000000005CD

Fichier Edition Fonctions Thèmes Disques Aide Language
Correct
31 °C
C: D:
Etat de Santé: Correct
Température: 32 °C

Rafraichir F5
Temps de l'Auto-Rafraichissement >
Options "Auto-Rafraichissement" >
Rescanner F6
Graphisme
Cacher le Numéro de Série
✓ Mettre en Barre de Tâches
✓ Démarrer avec Windows
Fonctionnalités Alertes >
Fonctionnalités Avancées >
Solution Bug Firmware >
Ouvrir "Gestion des Disques"
Ouvrir "Gestionnaire de Périphériques"

1 min.
3 min.
5 min.
• 10 min.
30 min.
60 min.
120 min.
180 min.
360 min.
720 min.
1440 min.
Désactiver

ID	Déta...			
01	Taux...		99	6
03	Temp...		98	0
04	Décompte des cycles de mise en rotation	98	98	20
05	Nombre de secteurs réalloués	100	100	36

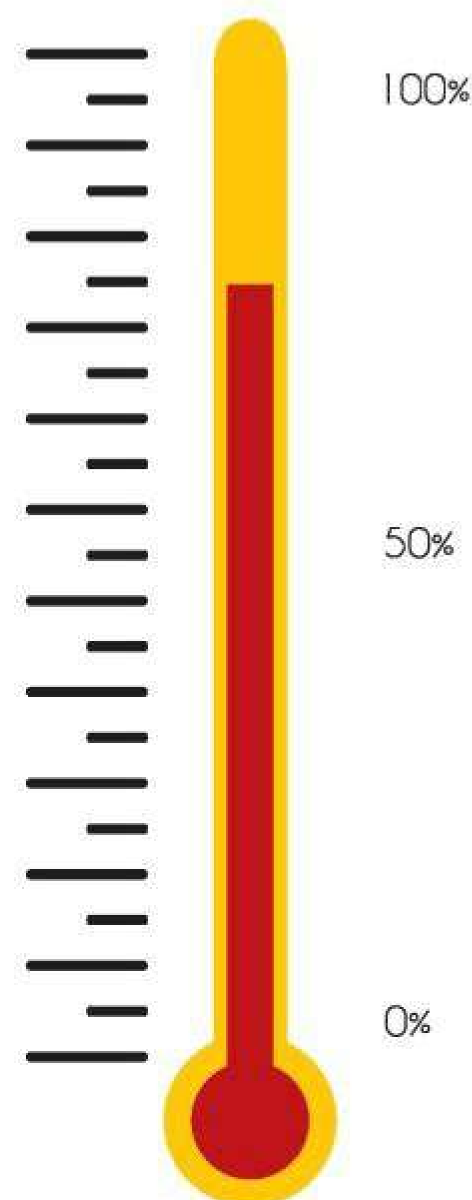
01 › FAIRE UN BILAN

CrystalDiskInfo présente le « bilan de santé » de vos disques durs. Vous naviguez entre ces derniers en cliquant sur les lettres correspondantes (**C:**, **F:** ...) en dessous de **Fichier**. L'état va de **Correct** (bleu clair) à **Mauvais** (rouge). Pour connaître les faiblesses de vos disques, consultez le tableau en bas de la fenêtre principale.

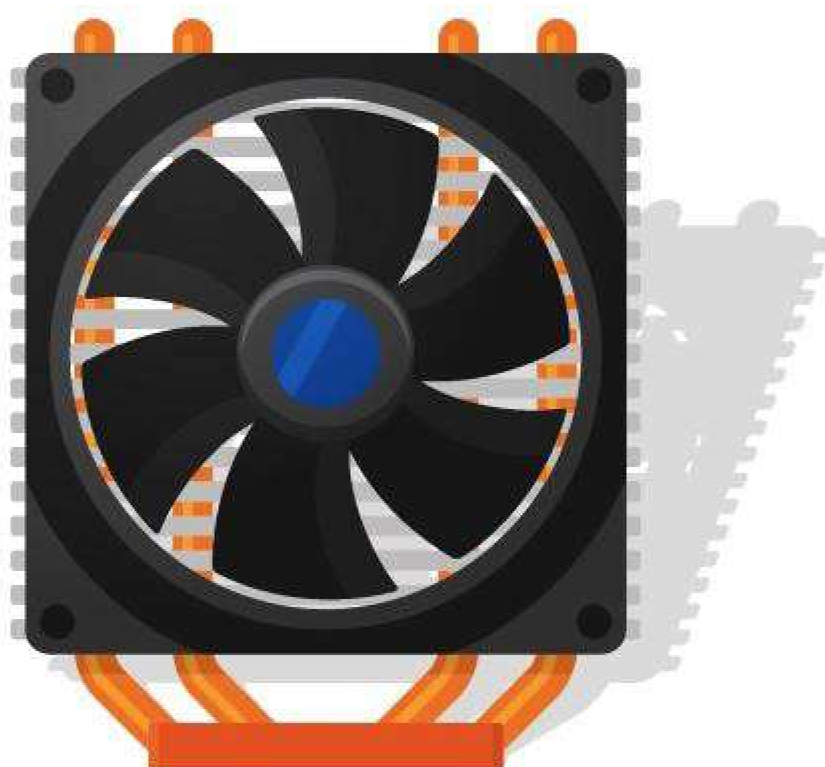
02 › SURVEILLER LES DISQUES

Pour surveiller vos disques durs de façon permanente, faites tourner le logiciel en arrière-plan (**Fonctions>Mettre en barre de tâches** et **Démarrer avec Windows**) et privilégiez un **Temps de l'Auto-Rafraîchissement** assez court. Les rapports sont ainsi plus fréquents.

MAÎTRISEZ LA TEMPÉRATURE DE VOTRE PC



La température a un impact direct sur les performances des composants. Une surchauffe peut provoquer des dysfonctionnements.



Le processeur (CPU), les disques durs ou la carte graphique (GPU) peuvent générer des erreurs ou se bloquer si leur température augmente de façon excessive. Tout ce petit monde constitue une chaudière qui surchaufferait en quelques minutes sans dispositif de refroidissement, radiateurs métalliques pour dissiper la chaleur et ventirads pour ventiler les composants. Vérifiez la température de votre PC avec SpeedFan, et entretenez régulièrement le circuit de refroidissement. Cela améliorera la longévité des composants, et réduira les risques de dysfonctionnement.

LIENS UTILES

Le site CPU-World (**www.cpu-world.com**) est une base de données très précieuse. Vous y trouverez votre modèle, la famille de processeurs et toutes les données techniques comme les températures minimum et maximum d'utilisation de votre CPU. Vous pouvez aussi consulter les catalogues d'Intel (**http://ark.intel.com**) ou d'AMD (**http://products.amd.com**).

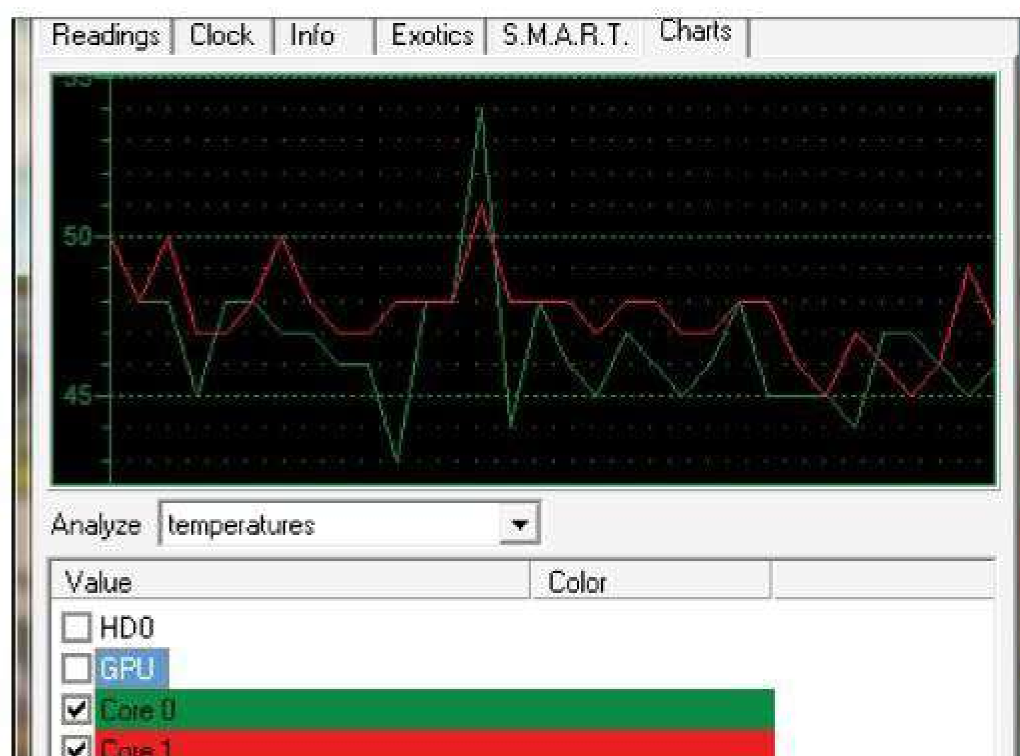


INFOS **[SPEEDFAN]** TUTO

Où le trouver ? [**www.almico.com/speedfan.php**] Difficulté :

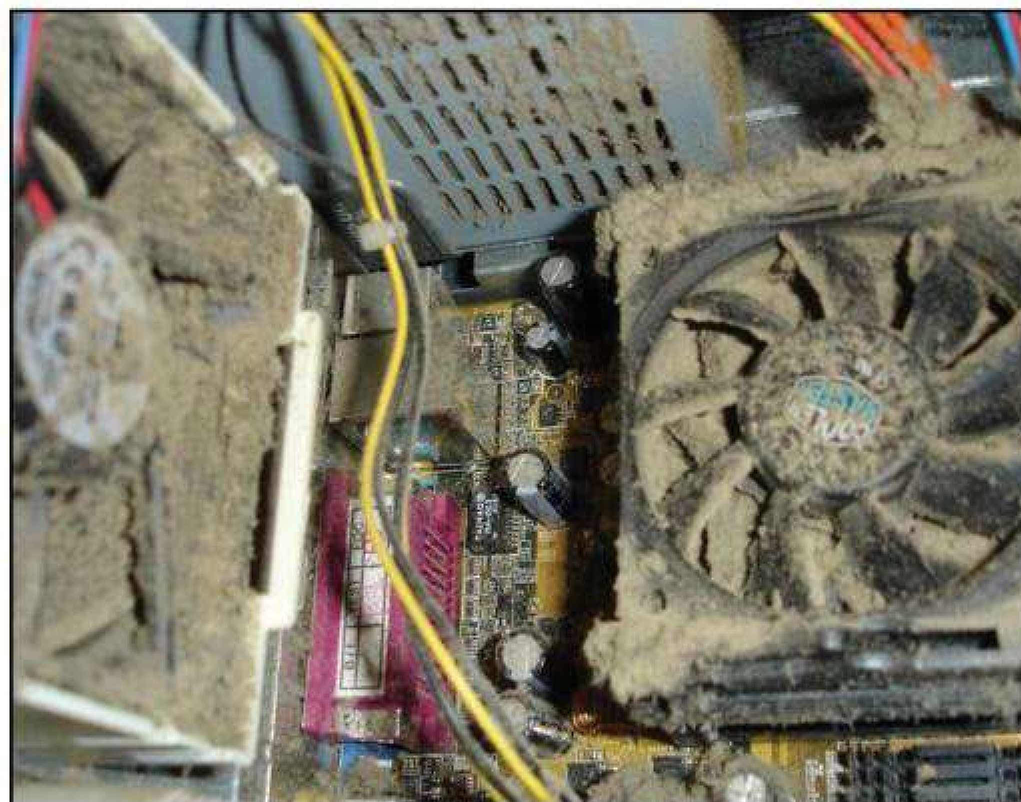
01 › PRENDRE LA TEMPÉRATURE

Le logiciel SpeedFan vous donnera les températures relevées par les différentes sondes thermiques de votre carte mère. Il est aussi en mesure d'accéder aux informations SMART des disques durs pour afficher leurs températures. Vous pourrez aussi contrôler la vitesse des ventilateurs en fonction de la chaleur, car n'oubliez pas que les composants seront différemment sollicités en fonction de l'utilisation que vous faites de votre PC.



02 › NETTOYER L'ORDINATEUR

Si votre PC est trop chaud, commencez par un bon nettoyage ! En effet, la poussière empêche la dissipation de la chaleur. Ouvrez le PC et nettoyez tout ce que vous pouvez avec coton-tige, aspirateur, bombe d'air comprimé, en prenant soin de décrasser les pales et les grilles des ventirads.



03 › AMÉLIORER LE REFROIDISSEMENT

Les ventirads et les extracteurs fatiguent au bout de quelques années d'usage intensif. En plus, ce type de matériel est souvent bas de gamme sur les PC vendus prêts à l'emploi, même chez les grandes marques. Vous pourrez par exemple remplacer le ventirad du CPU par un plus puissant et ajouter/changer un extracteur. On en trouve à tous les prix (de 10 à 80 €).





REMPLACEZ LES COMPOSANTS DÉFAILLANTS

Changer un composant défaillant n'est pas compliqué : une fois la pièce identifiée, il suffit généralement de démonter ou débrancher l'ancienne et de remettre la nouvelle en place à l'identique. Prenez juste soin de bien débrancher l'ordinateur avant de l'ouvrir !

CARTE MÈRE

C'est cette grande plaque électronique où sont placés tous les fils et les composants. C'est aussi le composant le plus long à remplacer puisqu'il faut tout démonter. C'est heureusement très rare.

ALIMENTATION

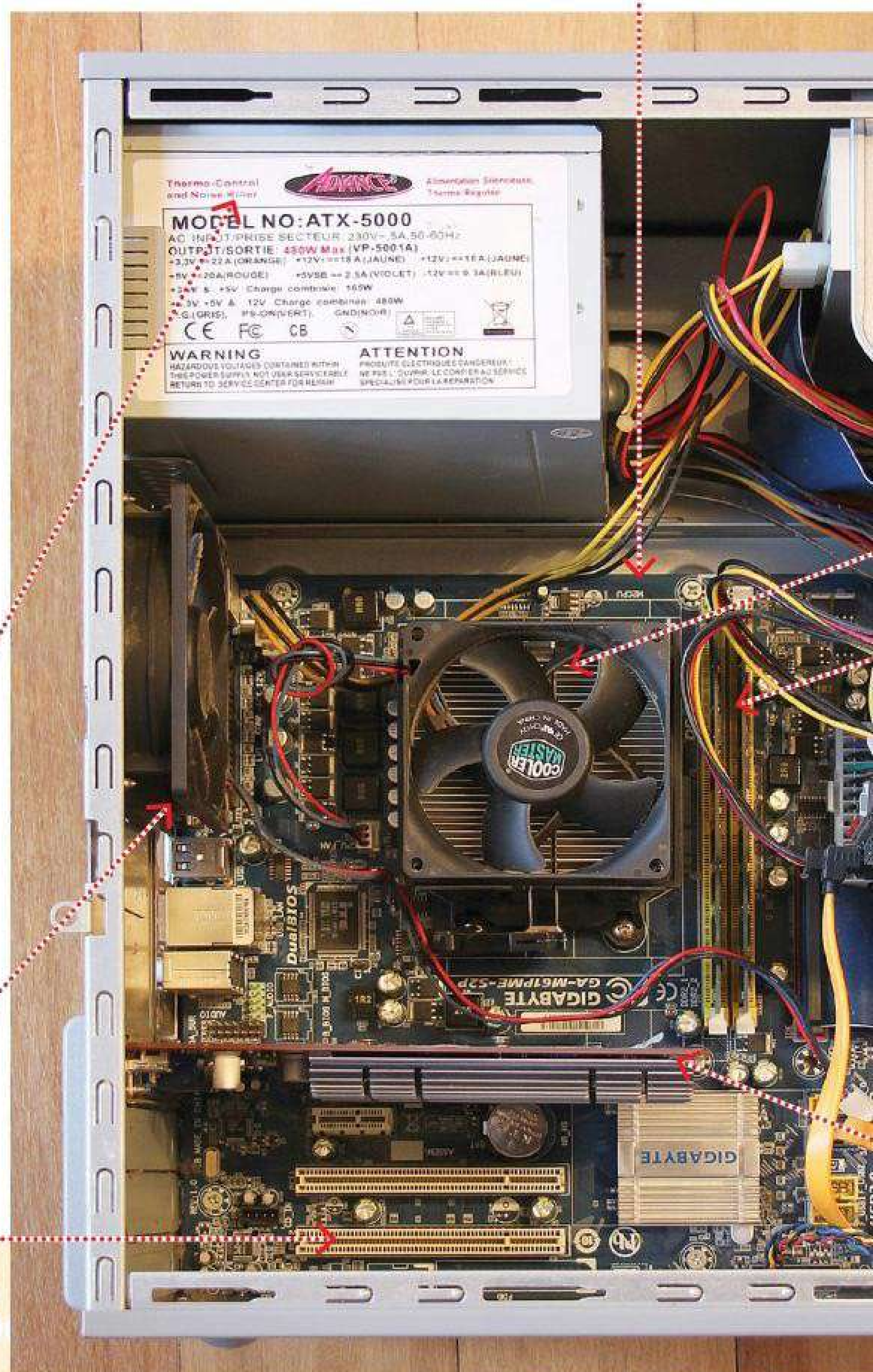
Si vous appuyez sur le bouton ON/OFF de votre ordinateur et qu'il ne fait pas un bruit c'est que l'alimentation a dû céder : coup de chaud, foudre ou vieillesse. En cas de problème, démontez-la, notez la référence et la puissance en Watts ou emmenez-la chez votre assembleur qui vous conseillera.

EXTRACTEUR

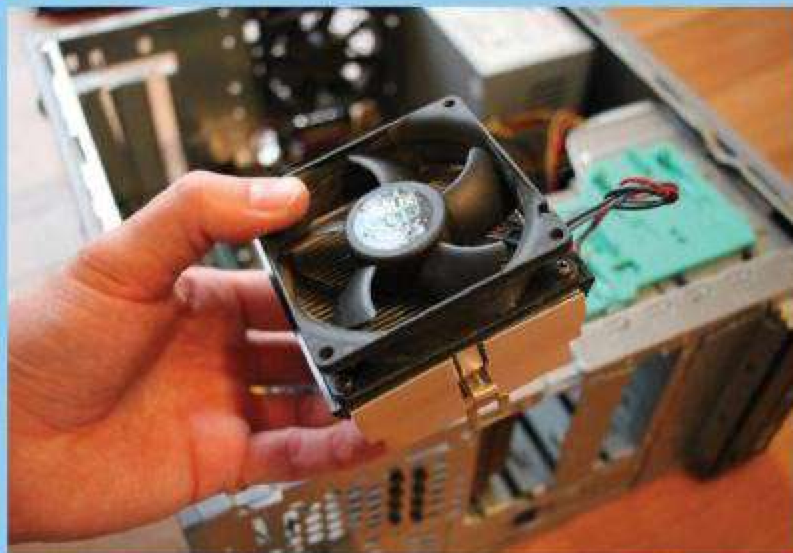
C'est un ventilateur monté à l'envers pour expulser l'air chaud vers l'extérieur du PC.

PORTS PCI

Ces ports permettent d'ajouter des cartes filles (carte son, d'acquisition, réseau, etc.) Elles sont ici inutilisées, car la carte mère intègre déjà tout ce qu'il faut pour fonctionner (chipset réseau et sonore).



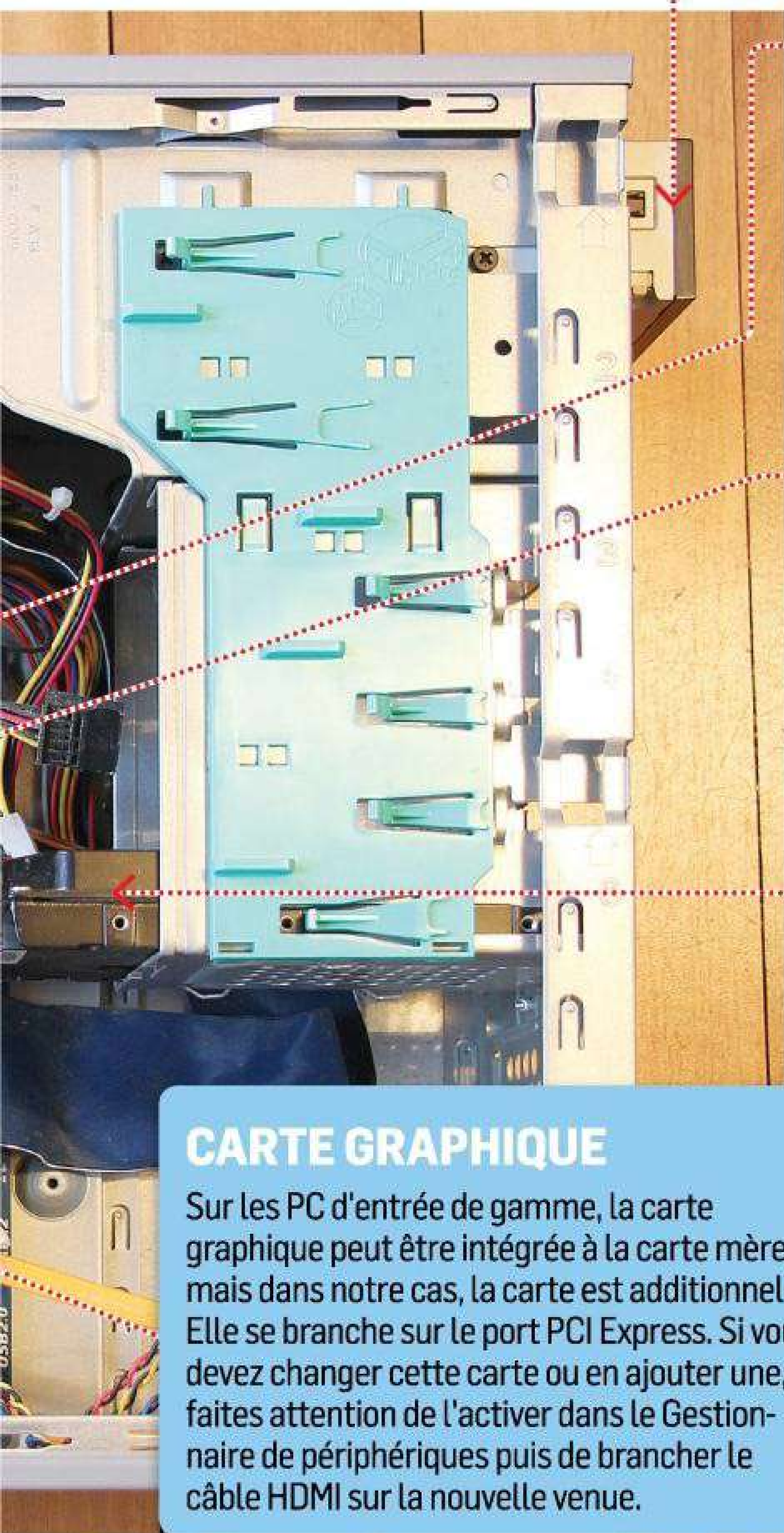
PROCESSEUR



Derrière le duo ventilateur-radiateur se cache le processeur enfiché dans son "socket". Un processeur ne «casse» jamais à moins de le faire fonctionner trop longtemps à des températures trop élevées (voir page précédente sur les problèmes de refroidissement). Mais peut-être voulez-vous simplement le changer pour en mettre un plus puissant ? Après avoir retiré le ventirad, actionnez le levier ZIF et enlevez délicatement le CPU. Attention, il faut que le nouveau soit compatible avec le «socket». Renseignez-vous avant d'acheter !

LECTEUR/ GRAVEUR DVD

Comme le disque dur, il est alimenté par une fiche et les données transitent par une autre au format IDE (PATA) ou SATA.



MÉMOIRE VIVE

Changer la RAM n'est pas très difficile, cela s'emboîte comme un Lego... à condition d'avoir le bon modèle. Il existe en effet plusieurs types de mémoire vive : DDR2, DDR3, DDR4 et encore plus si votre PC est ancien. Pour chaque type, il y a aussi la fréquence du bus à prendre en compte. Il faut avant tout noter la référence avant d'acheter ou aller chez son assembleur.

DISQUE DUR



Le disque dur est alimenté par une fiche provenant du bloc d'alimentation et l'échange des données avec la carte mère est assuré par un câble SATA (ici en orange). Le disque dur est le plus souvent vissé sur le châssis, mais il existe aussi des systèmes à clips. Pour le remplacer, il suffit de le retirer et de mettre le nouveau au même emplacement avec les mêmes câbles. Si vous n'avez qu'un disque dur interne, pas besoin de se soucier de la position des cavaliers master/slave.

CARTE GRAPHIQUE

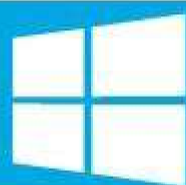
Sur les PC d'entrée de gamme, la carte graphique peut être intégrée à la carte mère, mais dans notre cas, la carte est additionnelle. Elle se branche sur le port PCI Express. Si vous devez changer cette carte ou en ajouter une, faites attention de l'activer dans le Gestionnaire de périphériques puis de brancher le câble HDMI sur la nouvelle venue.



SOULAGEZ VOTRE DISQUE SYSTÈME

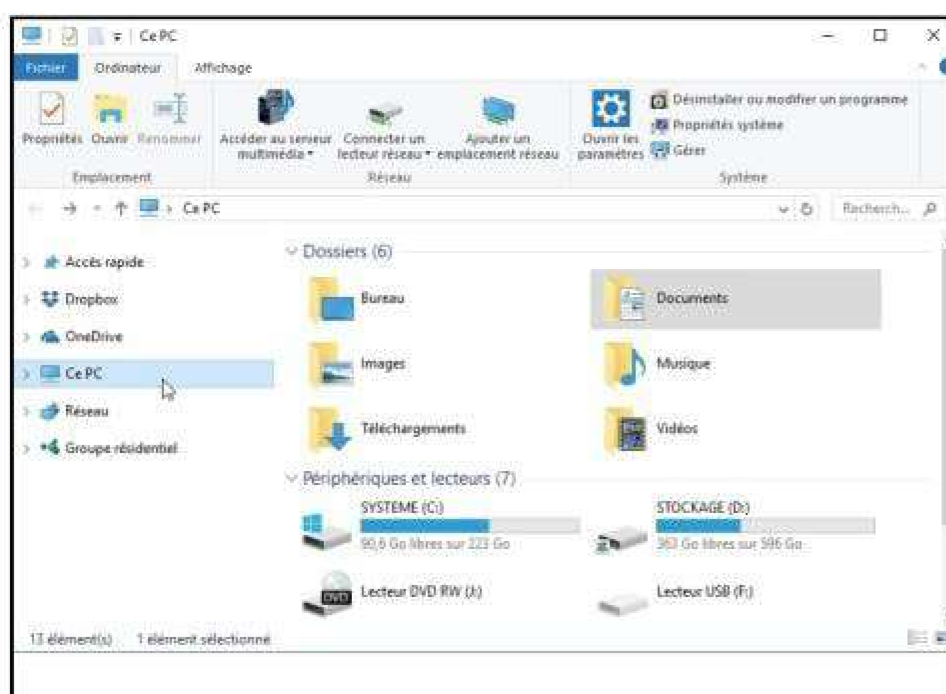


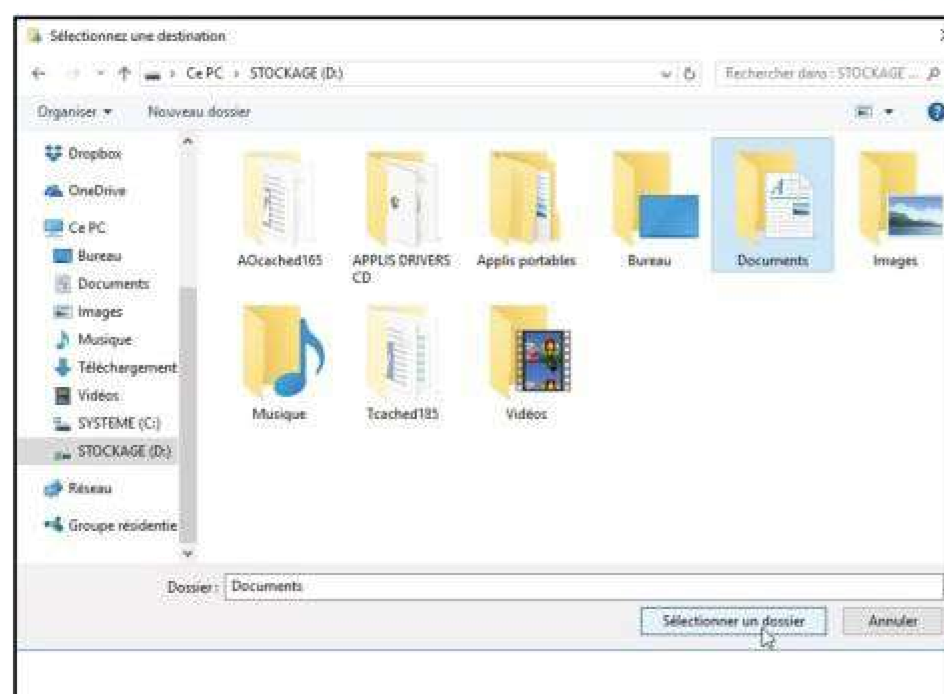
Votre disque sature ? Le remplacer implique de réinstaller Windows. Plus simple : ajouter un disque dur, et placer vos dossiers d'utilisateur dessus.



INFOS [WINDOWS] Difficulté :

TUTO





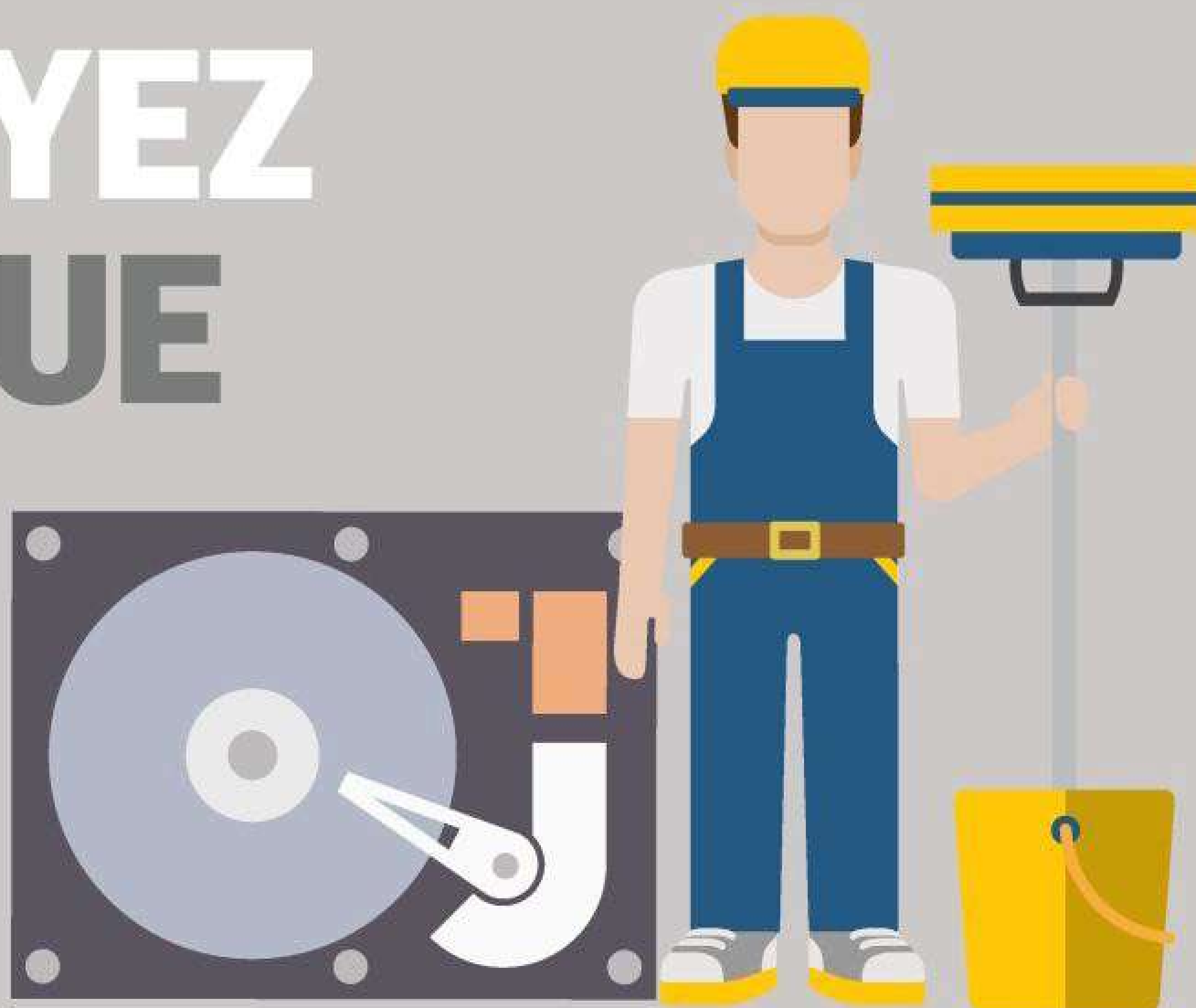
01 › TROUVER LES DOSSIERS

Ouvrez l'Explorateur de fichiers, et sélectionnez **Ce PC**, à gauche. Vous trouvez vos dossiers d'utilisateur : **Documents**, **Images**, **Musique**, etc. Faites un clic droit sur celui que vous désirez déplacer et choisissez **Propriétés>E mplacement>Déplacer**.

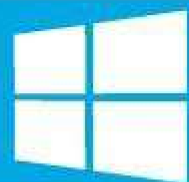
02 › INDIQUER L'EMPLACEMENT

Sélectionnez le disque de destination, à gauche, sous **Ce PC**, puis faites un clic droit dans la partie droite de la fenêtre et **Nouveau>Dossier**. Donnez-lui de préférence le même nom que le dossier d'origine (par exemple, **Documents**), puis sélectionnez-le et cliquez sur **Sélectionner un dossier**. Cliquez ensuite sur **OK** puis sur **Oui**.

NETTOYEZ LE DISQUE DUR

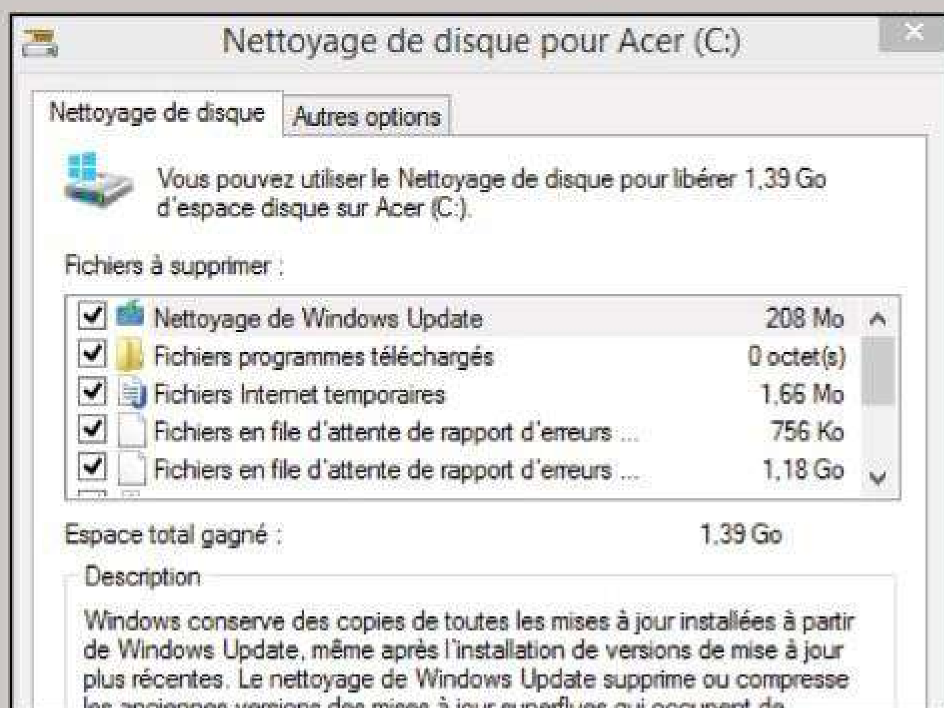


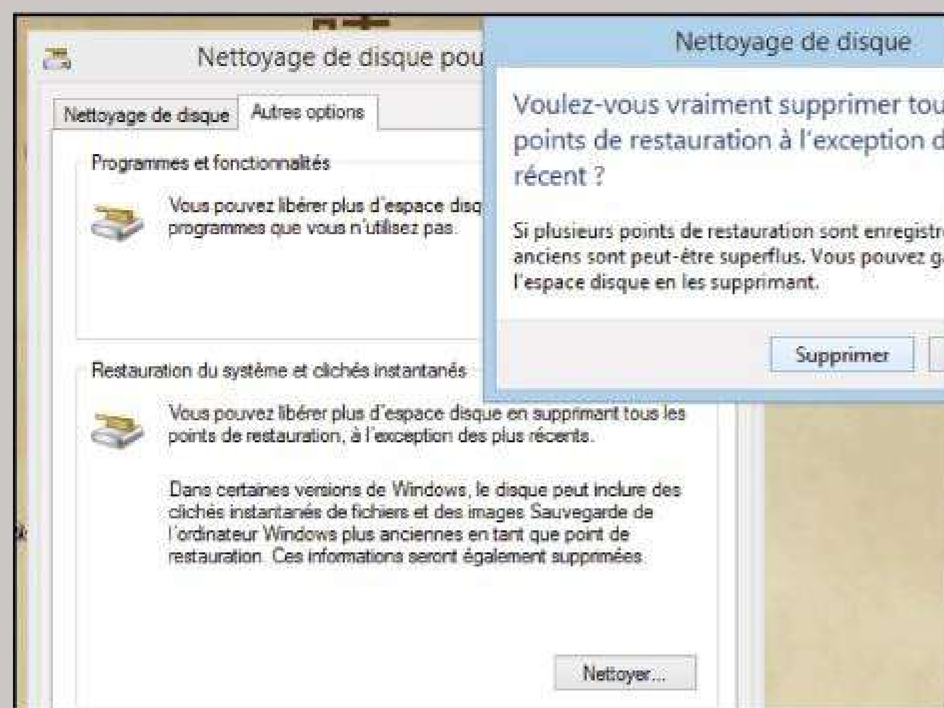
Outre le manque de place, la saturation d'un disque dur provoque un ralentissement des accès.



INFOS [WINDOWS] Difficulté :

TUTO





01 › SUPPRIMER LES FICHIERS INUTILES

Faites un clic droit sur le disque à nettoyer (**C:** est celui qui en a le plus besoin) puis **Propriétés > Nettoyage de disque**. Une fois l'analyse terminée, cliquez sur **Nettoyer les fichiers système**. Cochez toutes les cases dans la liste **Fichiers à supprimer**.

02 › SUPPRIMER LES ANCIENS POINTS DE RESTAURATION

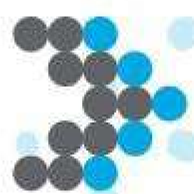
Allez maintenant dans l'onglet **Autres options** et cliquez sur **Nettoyer** en dessous de **Restauration du système et clichés instantanés**. Validez avec **Supprimer**. Retournez ensuite dans l'onglet **Nettoyage de disque** et terminez l'opération avec **OK > Supprimer les fichiers**.

METTEZ LES PILOTES À JOUR

Les pilotes logiciels qui gèrent les composants et périphériques de votre ordinateur peuvent être eux-mêmes à l'origine de dysfonctionnements.



Dans un PC, chaque composant matériel (disque dur, carte graphique, etc.), chaque périphérique (imprimante, webcam, etc.), fonctionne avec Windows grâce à un petit logiciel qui le guide dans son intégration au système : le pilote. Un pilote inadapté ou victime d'un bug peut entraver le fonctionnement du matériel. En cas de souci avec un élément matériel, essayez une mise à jour du pilote. Vous pouvez consulter le site Web du fabricant, comme nous l'avons vu dans le cas de la carte graphique, passer par le Gestionnaire de périphériques de Windows, ou bien recourir à un service spécialisé comme Driver Booster, détaillé ci-contre, qui vous mâche le travail.

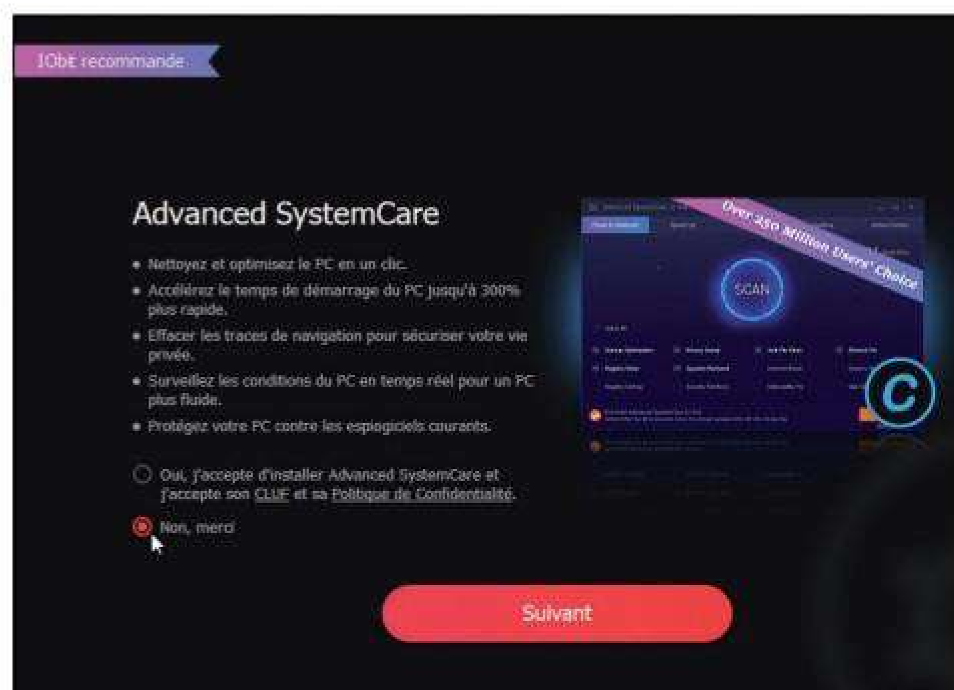


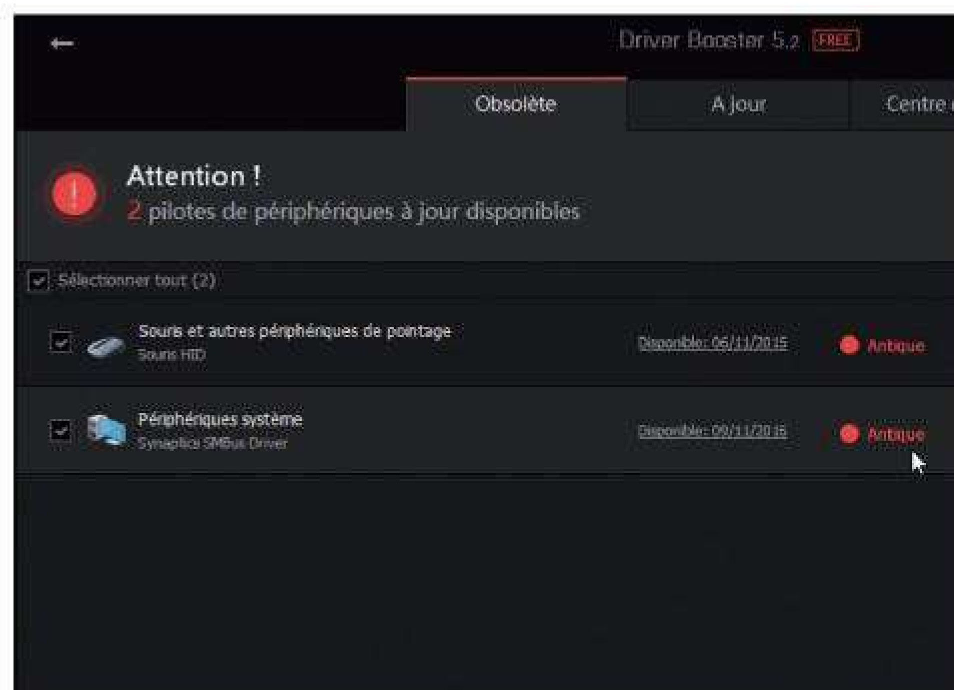
LA MISE À JOUR DES PILOTES PEUT AMÉLIORER LES PERFORMANCES DE VOTRE PC...



INFOS **[DRIVER BOOSTER]**
Où le trouver ? [**www.iobit.com**] Difficulté :

TUTO



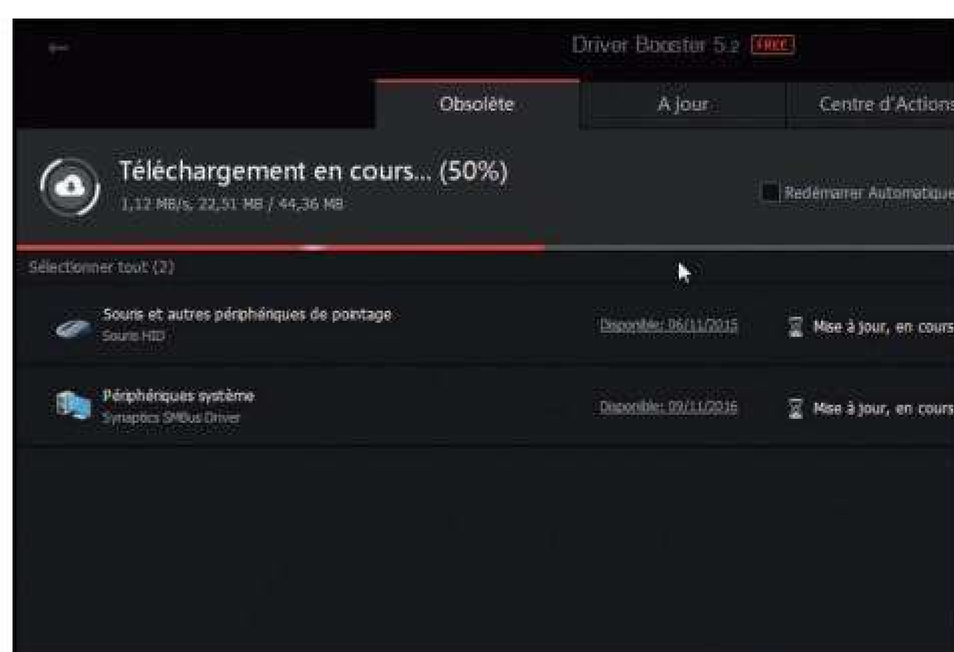


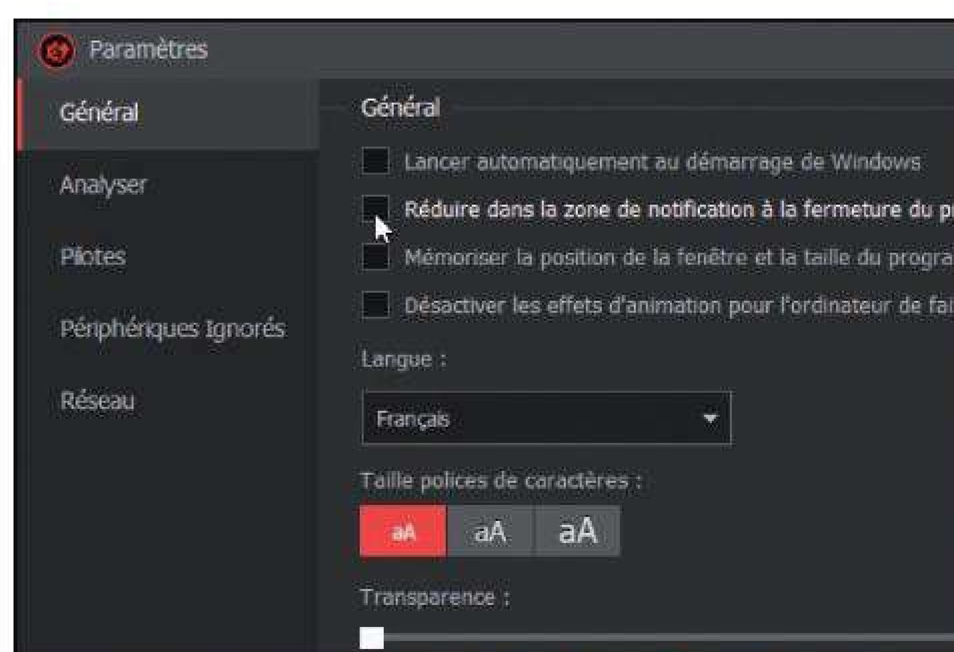
01 › INSTALLER

Lors de l'installation, Driver Booster vous propose un programme additionnel dont vous n'avez pas forcément besoin. Choisissez **Non, merci** dans la fenêtre proposant d'installer Advanced SystemCare Free. Cliquez ensuite sur **Suivant**, et patientez jusqu'à la fin de l'installation. De même, déclinez l'abonnement à la newsletter.

02 › ANALYSER

À l'issue de l'installation, Driver Booster effectue automatiquement une analyse de tous les pilotes installés sur votre système. Celle-ci achevée, il affiche la liste de tous les pilotes pour lesquels une nouvelle version est disponible (mention **Antique**), et que vous pouvez donc **Mettre à jour**.





03 › METTRE À JOUR

Plutôt que de **Mettre à jour** un à un chaque pilote, cochez, à l'aide des cases placées à gauche de l'interface, ceux qui vous intéressent, puis choisissez **Mettre à jour maintenant** pour effectuer une mise à jour groupée. Les pilotes sont alors téléchargés et installés. La création d'un point de restauration Windows est automatique.

04 › QUITTER

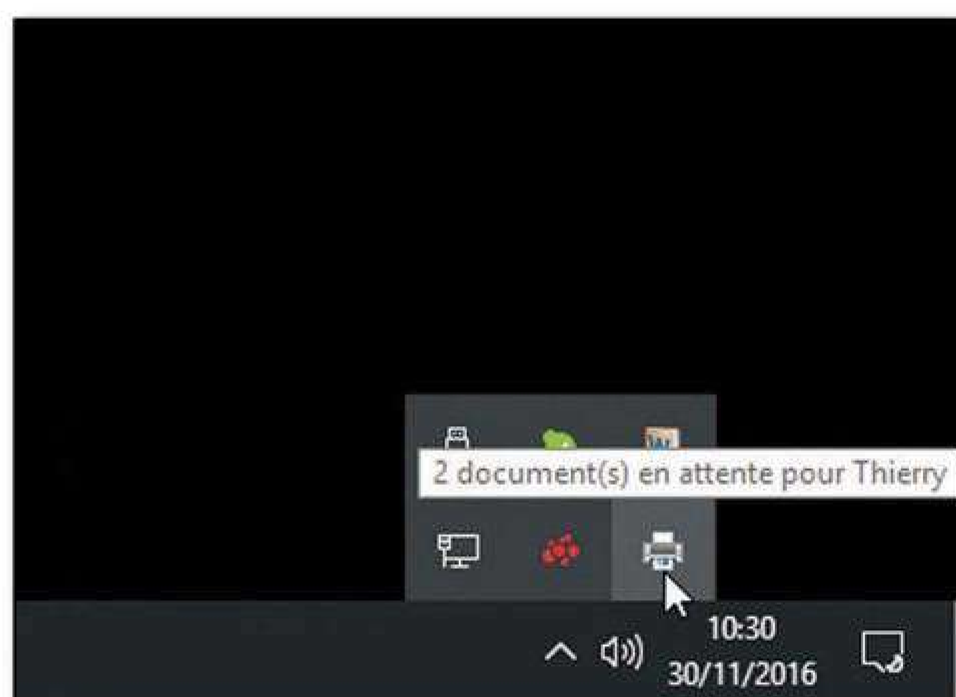
Lorsque vous refermez Driver Booster, il reste en veille en tâche de fond. Pour éviter cela à l'avenir, faites un clic droit sur son icône, à l'extrémité de la barre des tâches, choisissez **Paramètres** et décochez **Réduire dans la zone de notification**... Cliquez sur **Appliquer**. Puis faites un clic droit sur l'icône et choisissez **Quitter**.

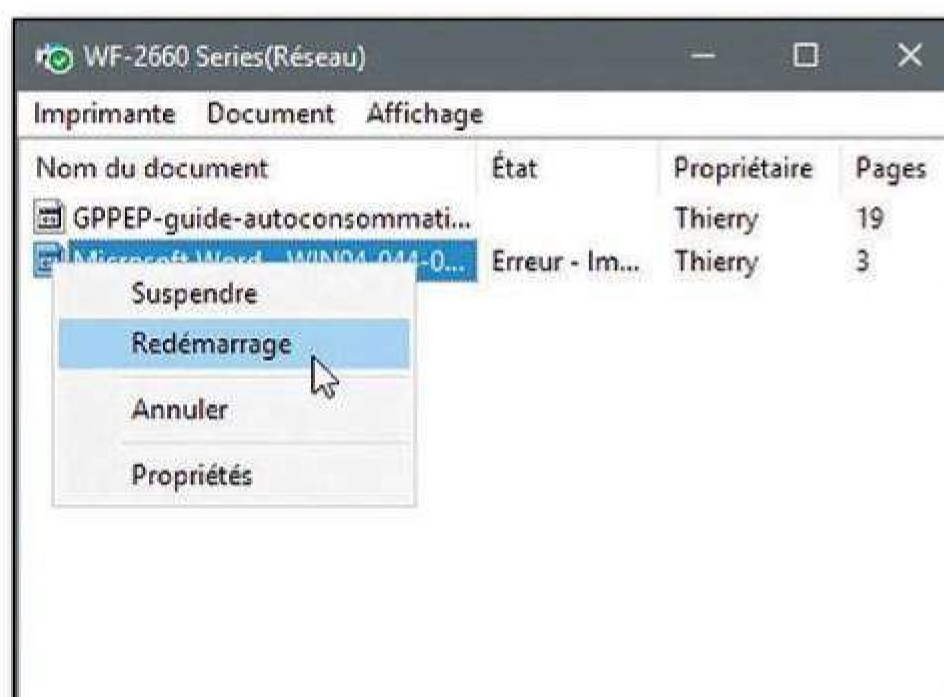
DÉBLOQUEZ L'IMPRESSION

Vérifiez la file d'attente d'impression pour voir ce qui bloque ou supprimer les travaux inutiles.



 [WINDOWS] Difficulté : TUTO





01 › OUVRIR LA FILE D'ATTENTE

Une fois l'impression lancée, vous pouvez accéder à la file d'attente d'impression en faisant un double-clic sur la petite icône d'imprimante située à l'extrémité de la barre des tâches (si elle n'apparaît pas directement, cliquez sur la flèche vers le haut).

02 › GÉRER LES IMPRESSIONS

Faites un clic droit sur le document qui pose problème. Vous pouvez alors demander un **Redémarrage** de l'impression ou **Annuler** l'impression de ce document. Pour tout annuler, allez dans le menu **Imprimante** et choisissez **Annuler tous les documents**.

ENTRETENEZ VOTRE IMPRIMANTE

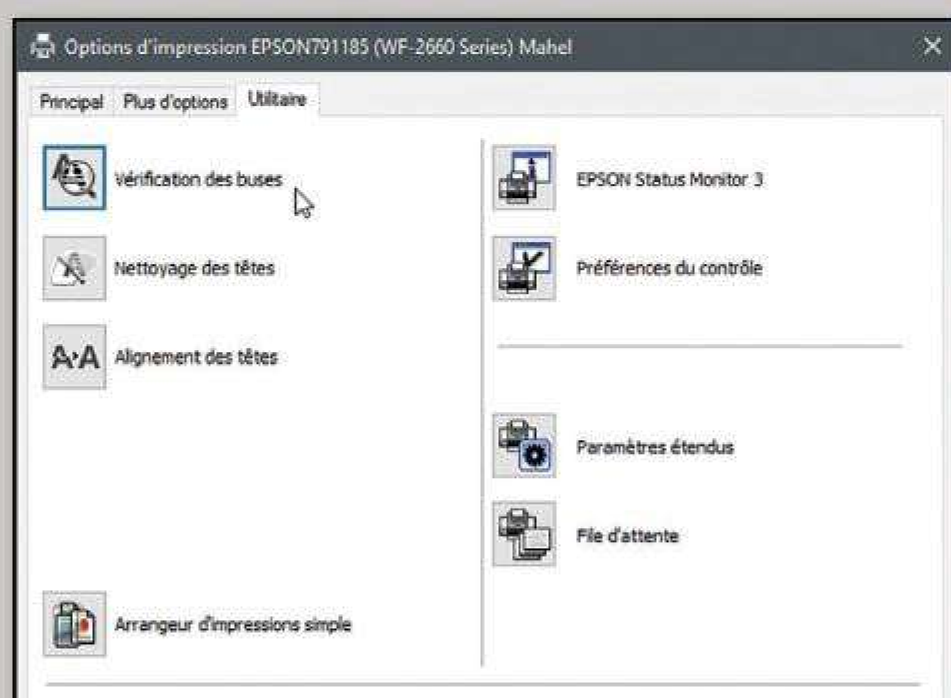


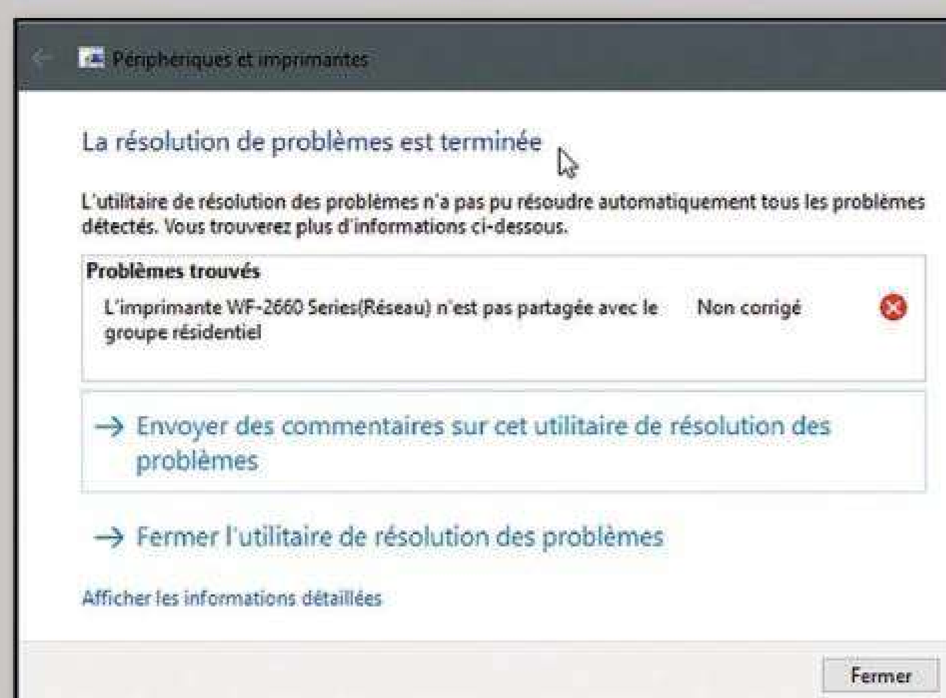
Lorsque la qualité se dégrade, un nettoyage des têtes d'impression s'impose. Si carrément l'imprimante ne fonctionne plus, essayez l'outil de résolution de problèmes.



INFOS [PILOTE D'IMPRIMANTE]
Difficulté : ☠☠☠

TUTO





01 › EFFECTUER LA MAINTENANCE

Dans le Panneau de configuration, ouvrez la section **Périphériques et imprimantes**. Faites un clic droit sur votre imprimante et **Options d'impression**. Ici, à l'onglet **Utilitaire** (cela dépend des modèles), on trouve les outils de maintenance. Procédez d'abord à une **Vérification des buses**, puis, en cas de besoin, à un **Nettoyage des têtes** (couleurs incorrectes) ou à un **Alignement des têtes** (décalages).

02 › ESSAYER L'UTILITAIRE WINDOWS

Si votre imprimante n'imprime carrément plus, après les vérifications d'usage (branchements, redémarrage de l'appareil), toujours dans la section **Périphériques et imprimantes**, faites un clic droit sur votre imprimante et **Résoudre les problèmes**. Déroulez la procédure, et appliquez le cas échéant les conseils qui vous sont délivrés. Résultat non garanti, mais à essayer.



01# Résoudre les problèmes de connexion Bluetooth

→ Avec les Paramètres

Votre PC est connecté, via Bluetooth, à un autre appareil, mais l'appairage ne produit aucun effet? L'association n'a pas fonctionné. Via le champ de recherche, tapez **Paramètres Bluetooth** pour les ouvrir. Vérifiez que le **Bluetooth** est bien **Activé** et que votre appareil est **Couplé**. Si cela ne fonctionne pas, choisissez de **Supprimer** l'appareil. Validez avec **Oui**, retentez de le **Jumeler**.

Difficulté :

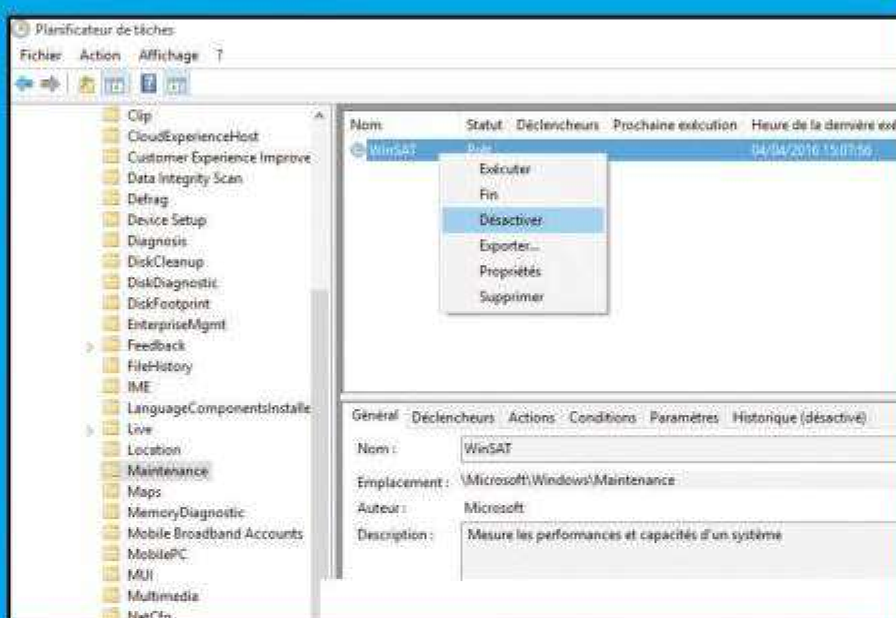


02# Désactiver les tests de performance

→ Avec le Planificateur de tâches

Régulièrement, votre PC ralentit tandis que le disque dur se met à fonctionner avec frénésie? Il s'agit de tests de performance effectués par Windows. Pour les désactiver, tapez **taskschd.msc** dans la barre de recherche et validez avec **Entrée**. Déroulez **Planificateur de tâches (Local)> Bibliothèque du Planificateur> Microsoft> Windows> Maintenance**. Faites un clic droit sur **WinSAT** et gauche sur **Désactiver**.

Difficulté :



03# Mettre à jour les pilotes

→ Avec le Gestionnaire de périphériques

Mettre à jour le pilote d'un périphérique est parfois la meilleure solution pour résoudre un problème. Vous pouvez le faire via le **Gestionnaire de périphériques**, accessible à partir du **Panneau de configuration** (ou via un clic droit sur le menu Démarrer, avec Windows 10). Faites un clic droit sur le périphérique en cause et cliquez sur **Mettre à jour le pilote**. Cliquez sur **Rechercher automatiquement un pilote mis à jour**. Si Windows ne trouve pas la mise à jour, à vous de télécharger le pilote sur le site du fabricant et de l'installer en cliquant cette fois-ci sur **Rechercher un pilote sur mon ordinateur**.



Difficulté :

04# Empêcher la mise à jour automatique des pilotes

→ AVEC LE PANNEAU DE CONFIGURATION



Windows Update est susceptible de procéder à la mise à jour des pilotes de votre matériel sans vous en informer, ce qui n'est pas forcément souhaitable (si une mise à jour peut résoudre un problème... elle peut aussi en causer s'il n'y en avait pas!). Pour éviter cela, ouvrez le Panneau de configuration, rubrique **Système**. Cliquez sur **Paramètres système avancés**. Sélectionnez l'onglet **Matériel** et cliquez sur **Paramètres d'installation des périphériques**. Cochez **Non** et validez avec **Enregistrer les modifications**.

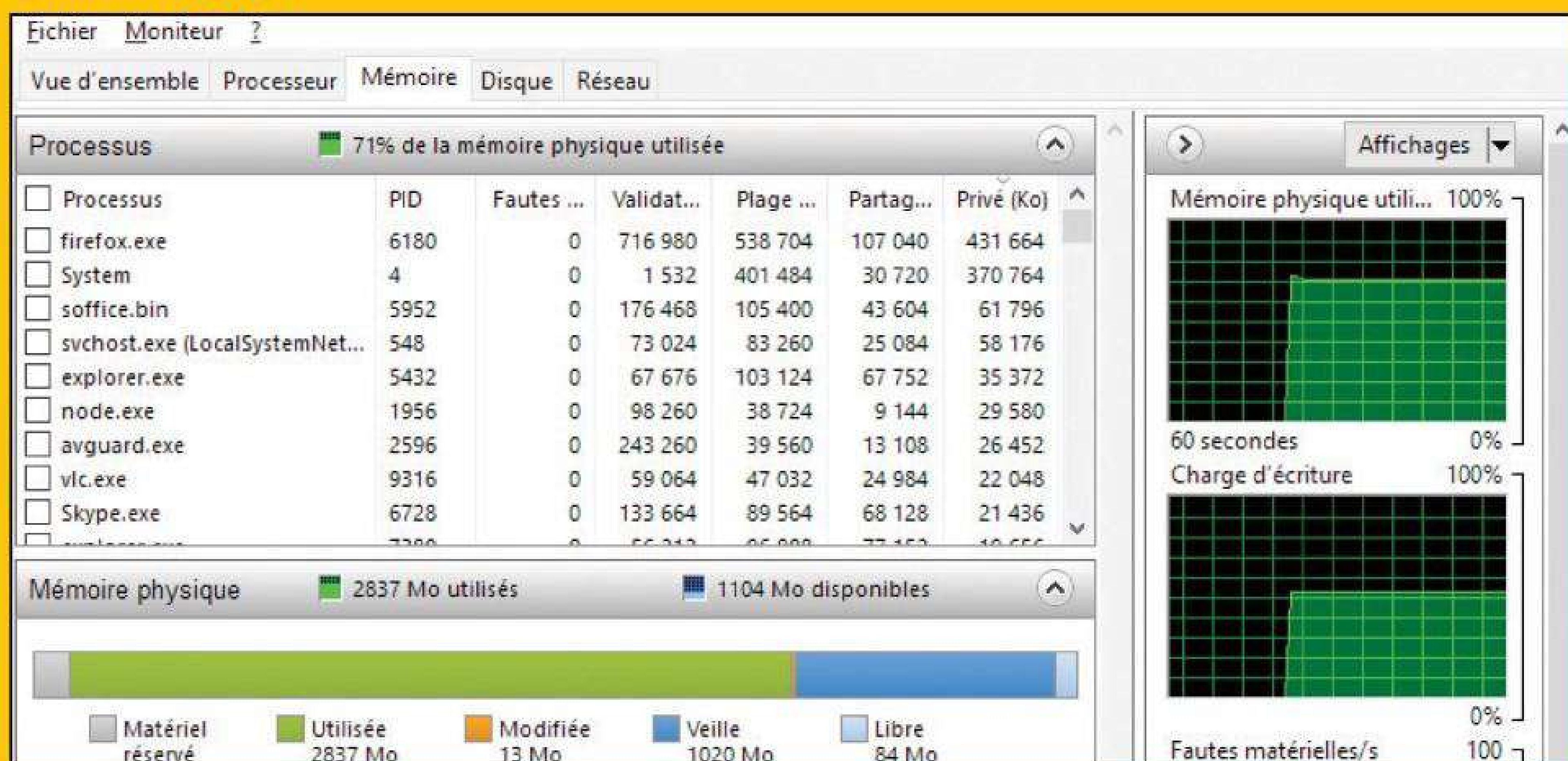
Difficulté :

05# Vérifier la charge de travail du PC

→ AVEC LE MONITEUR DE RESSOURCES WINDOWS

Le Moniteur de ressources de Windows permet d'avoir un aperçu de ce qui pèse sur votre système, votre RAM ou votre réseau. C'est le premier outil à consulter lorsque vous constatez une baisse des performances. Tapez sur la touche **Windows +R**, saisissez **resmon** et validez. L'onglet **Vue d'ensemble** donne un synthèse de la charge des composants, graphiques à l'appui, tandis que les onglets **Processeur**, **Mémoire** et **Disque** affichent l'utilisation moyenne de ces ressources pour chaque application.

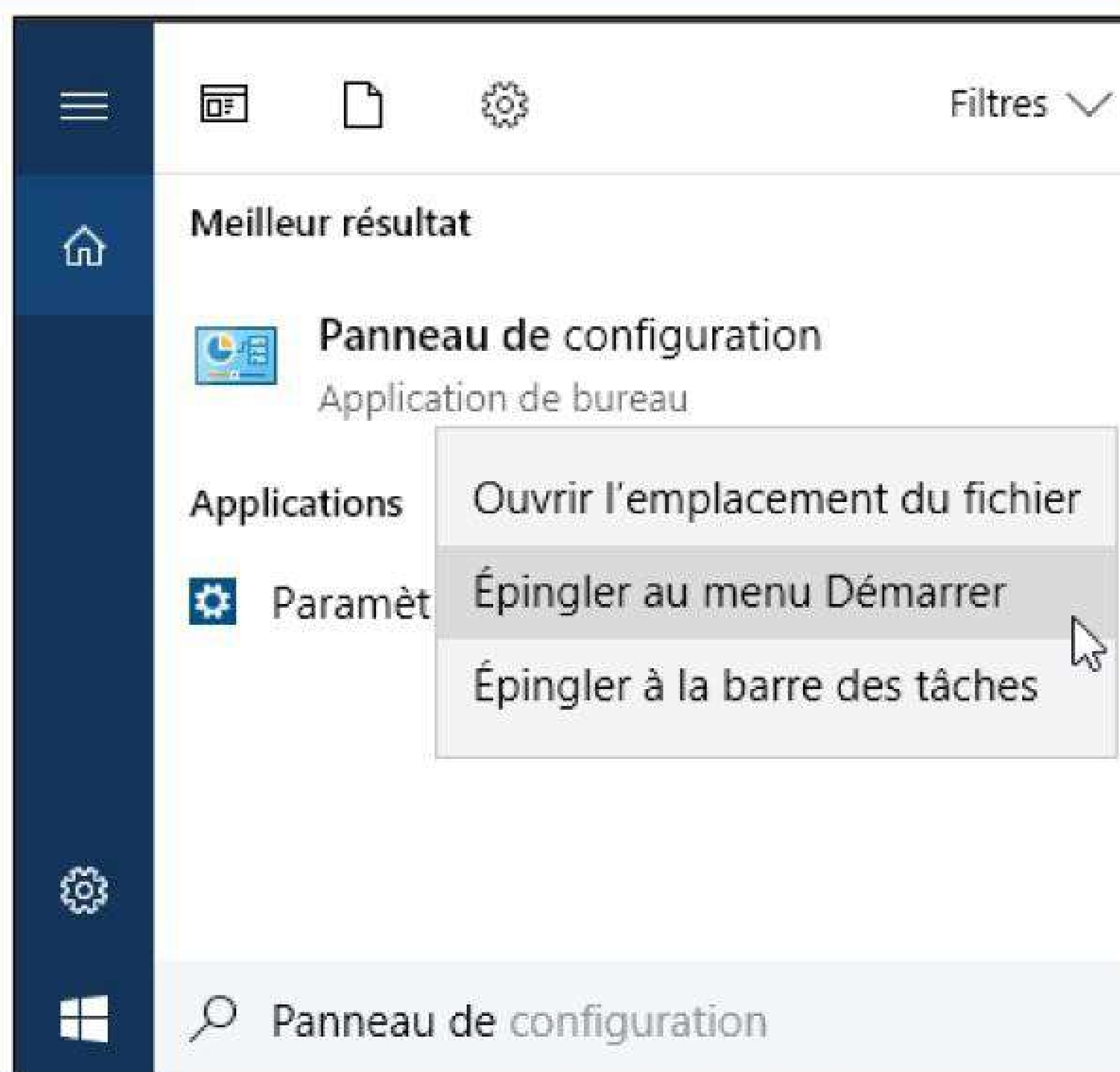
Difficulté :



06# Accéder au Panneau de configuration
→ Avec Windows 10

La dernière mouture de Windows bénéficie d'une nouvelle fenêtre des **Paramètres**, accessible via le menu Démarrer. Mais certaines options se règlent encore dans l'ancien Panneau de configuration, hérité des précédentes éditions. Pour y accéder, tapez simplement **Panneau de configuration**, dans la barre de recherche de Windows. Pour y accéder plus rapidement à l'avenir, faites un clic droit sur Panneau de configuration, dans la liste de résultats, et choisissez **Épingler au menu Démarrer**.

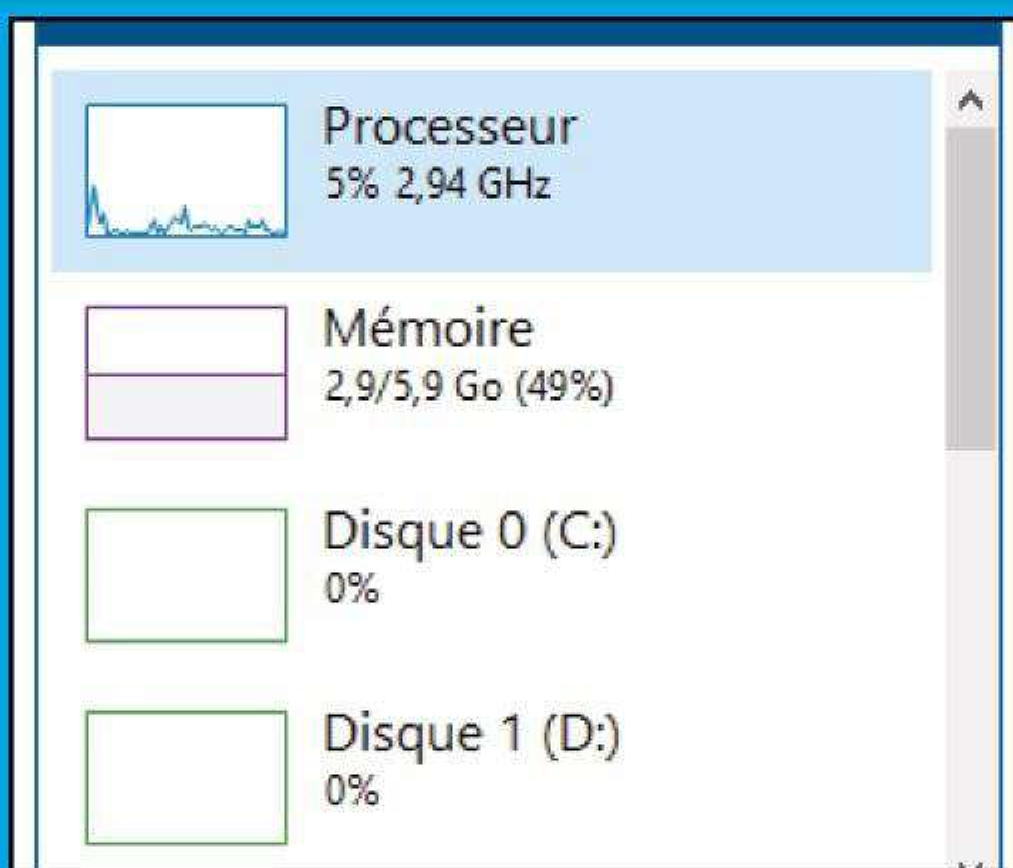
Difficulté :



07# Surveiller processeur et mémoire
→ Avec le Gestionnaire des tâches

Tapez la combinaison de touches **Ctrl+Alt+Suppr** et choisissez **Gestionnaire des tâches**. Allez à l'onglet **Performances**. Vous pouvez y suivre la charge de travail des différents composants de votre PC: processeur, mémoire, disque, etc. Faites un double-clic dans la colonne de gauche pour afficher un panneau réduit, que vous pouvez redimensionner à loisir et conserver sous les yeux pour surveiller l'activité des composants pendant que vous travaillez.

Difficulté :



08# Diagnostiquer sa batterie

→ Avec HWMonitor

Les batteries des ordinateurs vieillissent et après quelques années votre PC tient moins bien la charge. Si vous voulez faire le point sur votre batterie le logiciel HWMonitor dispose d'une fonctionnalité très utile: l'évaluation de sa capacité actuelle (**Current Capacity**). Cette donnée est bien sûr à comparer à la capacité d'origine (**Designed Capacity**). Dans notre exemple, la batterie de notre bon vieux PC datant de presque 5 ans n'a pas trop souffert: de 47 520 mWh,elle est passée à 39 042 soit une baisse de 18% (**Wear Level**).

Difficulté :

Lien : **http://goo.gl/NAXF**

CPUID HWMonitor

File View Tools Help

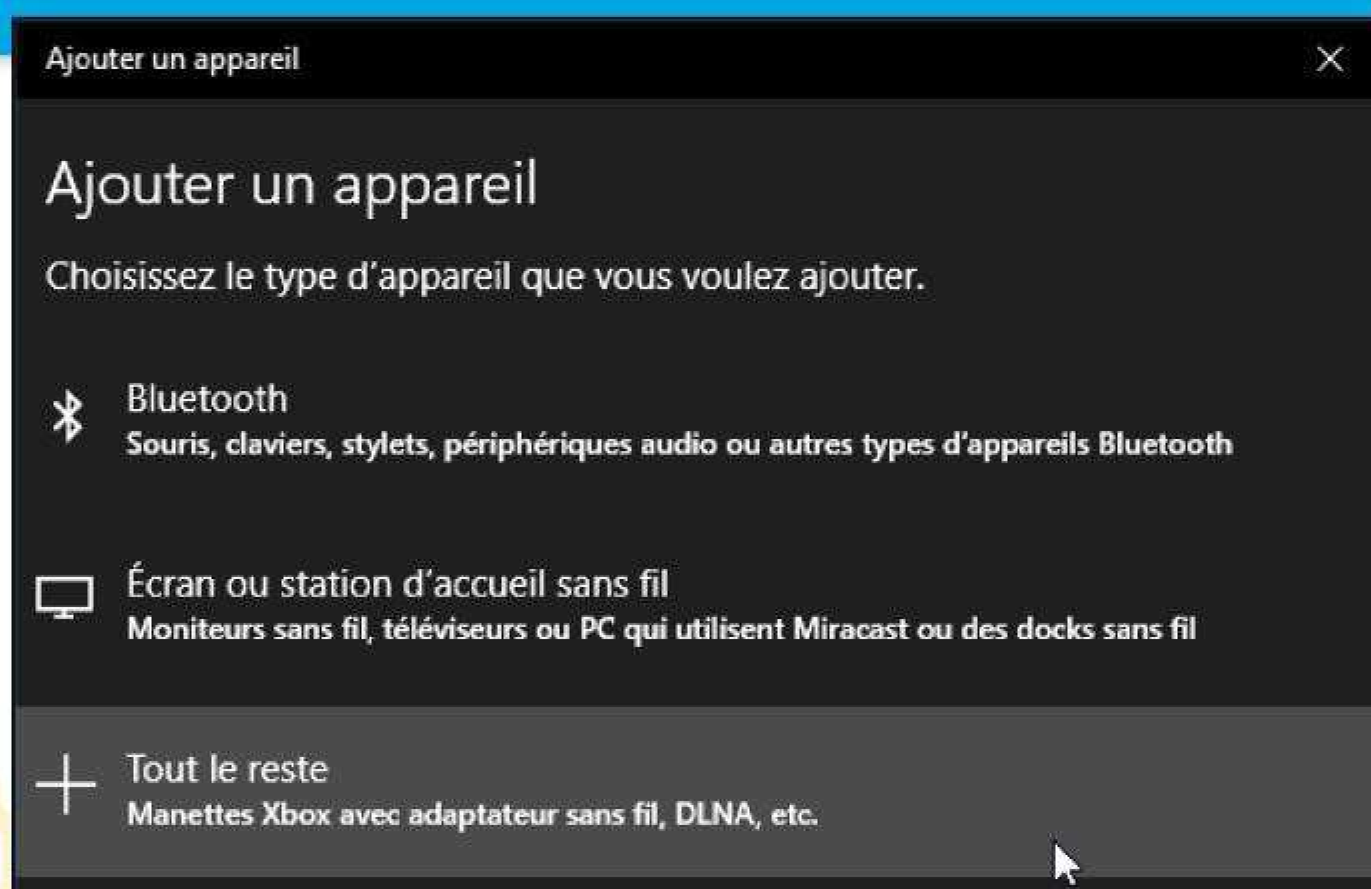
Sensor	Value	Min	Max
Temperatures			
Core #0	65 °C (149 °F)	62 °C (143 °F)	72 °C (161 °F)
Core #2	61 °C (141 °F)	61 °C (141 °F)	72 °C (161 °F)
Powers			
Package	25.00 W	1.25 W	25.00 W
Clocks			
Core #0	2527 MHz	2527 MHz	2528 MHz
Core #2	2527 MHz	2527 MHz	2528 MHz
Utilizations			
UC	7 %	4 %	56 %
CPU #0	10 %	4 %	52 %
CPU #1	6 %	0 %	56 %
CPU #4	6 %	0 %	52 %
CPU #5	6 %	1 %	64 %
TOSHIBA MK3265GSXN			
Temperatures			
Assembly	40 °C (104 °F)	40 °C (104 °F)	41 °C (105 °F)
AMD Mobility Radeon HD 50...			
Voltages			
VINO	1.120 V	0.950 V	1.120 V
Temperatures			
TMPIN0	71 °C (158 °F)	68 °C (154 °F)	72 °C (160 °F)
Clocks			
Graphics	750 MHz	157 MHz	750 MHz
Memory	800 MHz	305 MHz	800 MHz
Utilizations			
GPU	0 %	0 %	13 %
Battery			
Voltages			
Current Voltage	12.369 V	12.367 V	12.369 V
Capacities			
Designed Capacity	47520 mWh	47520 mWh	47520 mWh
Full Charge Capacity	39042 mWh	39042 mWh	39042 mWh
Current Capacity	39042 mWh	39042 mWh	39042 mWh
Levels			
Wear Level	18 %	18 %	18 %

09# Installer manuellement un périphérique

→ Avec Windows 10

En règle générale, Windows reconnaît automatiquement les nouveaux périphériques que vous ajoutez, et installe le pilote nécessaire. Si ce n'est pas le cas, faites **Paramètres**> **Périphériques**> **Appareils Bluetooth et autres**. Cliquez sur **Ajouter un appareil...** et suivez les instructions.

Difficulté :



BEST-OF APPLIS 2019

LE GUIDE DES APPLIS INDISPENSABLES... ET GRATUITES !

MINI PRIX 3,90 €

Android MT

Mobiles & Tablettes

AVRIL - JUIN 2019

+30 ASTUCES & TUTOS INCLUS

BEST-OF 2019

480 APPLIS GRATUITES !

TESTÉES APPROUVÉES !

+68 JEUX ADDICTIFS

31 TRAVAIL & BUREAUTIQUE

36 SÉCURITÉ & VIE PRIVÉE

36 SPORTS & SANTÉ

28 FUN & INSOLITE

51 VIDÉOS & MUSIQUE

ETC !

CHEZ VOTRE MARCHAND DE JOURNAUX

SYSTÈME



p34
ENTRETENEZ Windows régulièrement

p38
Point de **RESTAURATION** : revenez en arrière !

p40
Désinstallez une mise à jour récalcitrante

p42
RÉPAREZ ou réinstallez Windows

p48
Retrouvez vos **CLÉS ET NUMÉROS** de licence

p50
Changez le **BOOT** depuis le **BIOS**

p52
MICROFICHES

ENTRETENEZ WINDOWS RÉGULIÈREMENT

Windows devient poussif, le démarrage s'éternise, la mémoire sature ? Voici quelques vérifications, et des opérations de nettoyage à réaliser régulièrement.





INFOS [WINDOWS] Difficulté :

TUTO

- [x] Animations dans la barre des tâches
- [ ] Animer les fenêtres lors de leur réduction et de leur agrandissen
- [x] Faire défiler régulièrement la zone de liste
- [ ] Faire disparaître ou apparaître les infobulles
- [ ] Faire disparaître ou apparaître les menus
- [x] Lisser les polices écran
- [x] Utiliser des ombres pour le nom des icônes sur le Bureau

◯ Taille gérée par le système
◯ Aucun fichier d'échange

Taille totale du fichier d'échange pour tous les lect

Minimale autorisée :	16 Mo
Recommandée :	1400 Mo
Allouée actuellement :	4096 Mo

01 › ACCÉLÉRER L'AFFICHAGE

Tapez **paramètres système** dans le champ de recherche Windows et cliquez sur **Afficher les paramètres systèmes avancés**. Allez dans les **Paramètres des Performances** et décochez **Animer les fenêtres..., Faire disparaître ou apparaître les infobulles** et **Faire disparaître ou apparaître les menus**. Validez avec Appliquer puis **OK**.

02 › RÉGLER LA MÉMOIRE VIRTUELLE

Une partie du disque dur est utilisée pour faire office de mémoire vive, moins rapide que la vraie. Pour optimiser cette fonction, tapez **performances** dans le champ de recherche et cliquez sur **Régler l'apparence et les performances**. Allez dans **Avancé** puis **Modifier**. Cochez **Taille personnalisée** et entrez la valeur **Recommandée** dans les deux champs. Validez avec **Définir** puis **OK** et redémarrez.

03 › ACCÉLÉRER LE DÉMARRAGE

De nombreux programmes, pas forcément utiles, se lancent en même temps que le PC. Ouvrez le Gestionnaire des tâches (**Ctrl + Maj + Échap**) et, dans l'onglet **Démarrage**, sélectionnez les programmes inutiles et cliquez sur le bouton **Désactiver**.

04 › DÉFRAGMENTER LE DISQUE DUR

Normalement, la défragmentation du disque dur se fait automatiquement à intervalles réguliers, mais mieux vaut le vérifier. Ouvrez **Ce PC**, faites un clic droit sur **C:** et allez dans les **Propriétés**. Dans l'onglet **Optimiser**, vérifiez que l'**Optimisation planifiée** est Activé. Sinon, **Modifier les paramètres**.

05 › IDENTIFIER LES PROCESSUS GOURMANDS

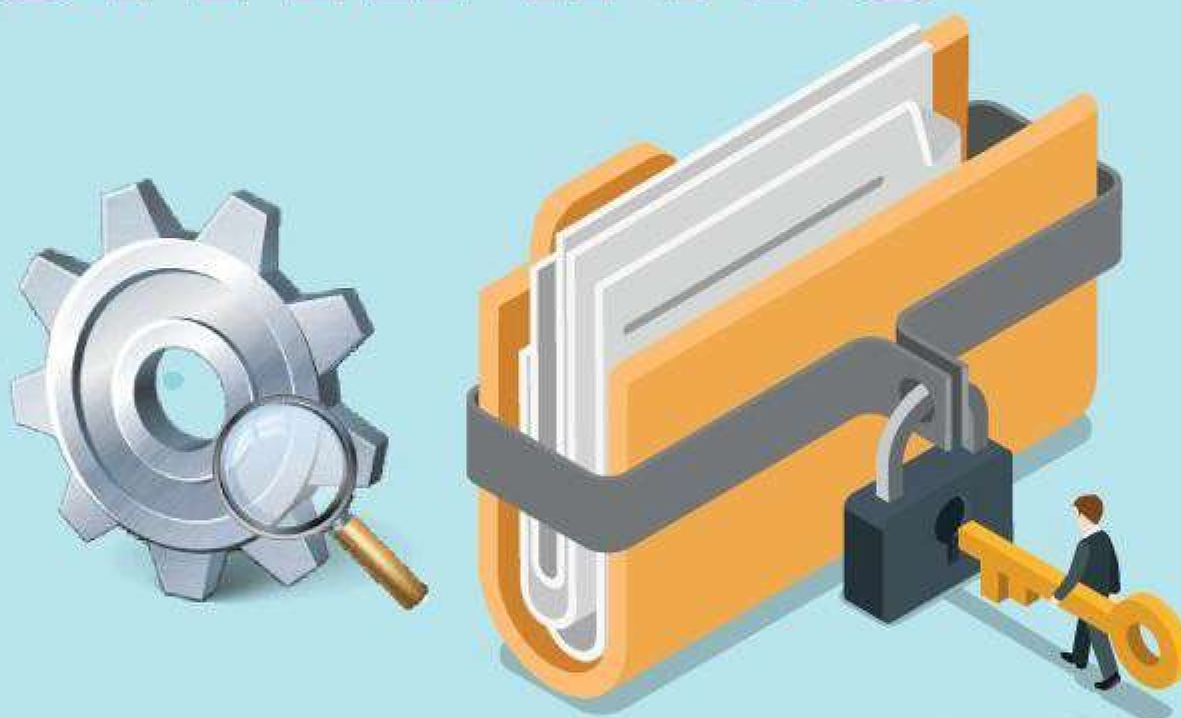
Certains de vos programmes consomment beaucoup de ressources, et ne vous sont pas très utiles. Dans le **Gestionnaire de tâches**, l'onglet **Processus** indique la consommation de mémoire des différents programmes. Vous pouvez en arrêter un avec un clic droit puis **Fin de tâche**. Pour une solution plus radicale, passez à l'étape suivante.

06 › DÉSINSTALLER LES PROGRAMMES INUTILES

Entre certaines applications préinstallées et les logiciels installés pour un usage ponctuel, la liste des programmes finit par s'allonger. Il est bon de la vérifier de temps en temps (**Paramètres du PC > Applications et fonctionnalités**)et de faire un clic droit pour **Désinstaller** ceux qui ne servent plus.

DÉBLOQUEZ LES FICHIERS RÉCALCITRANTS

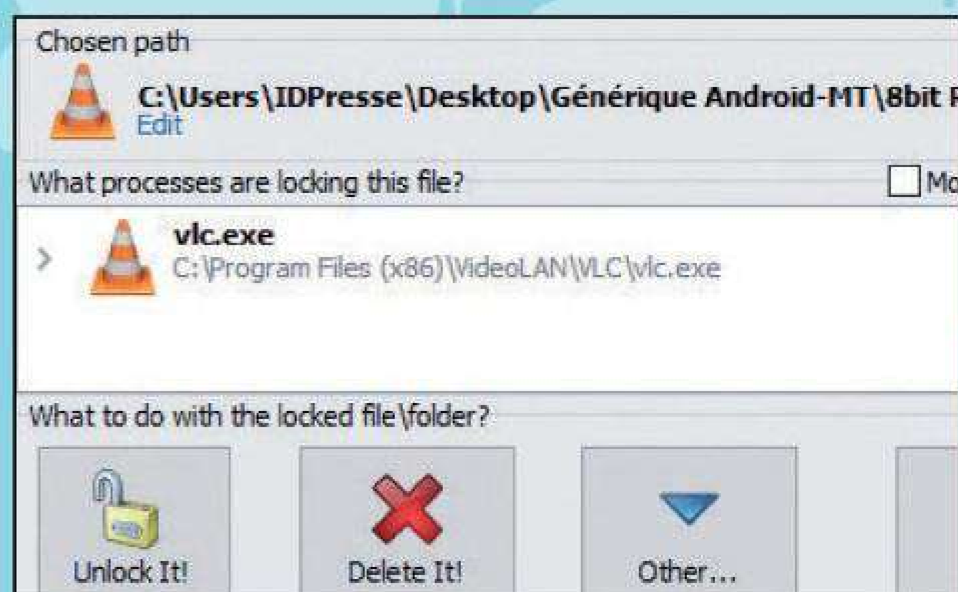
Impossible de supprimer un fichier parce qu'il est « déjà utilisé », mais vous ne savez pas par quoi ? LockHunter se charge de débusquer et d'arrêter le responsable.

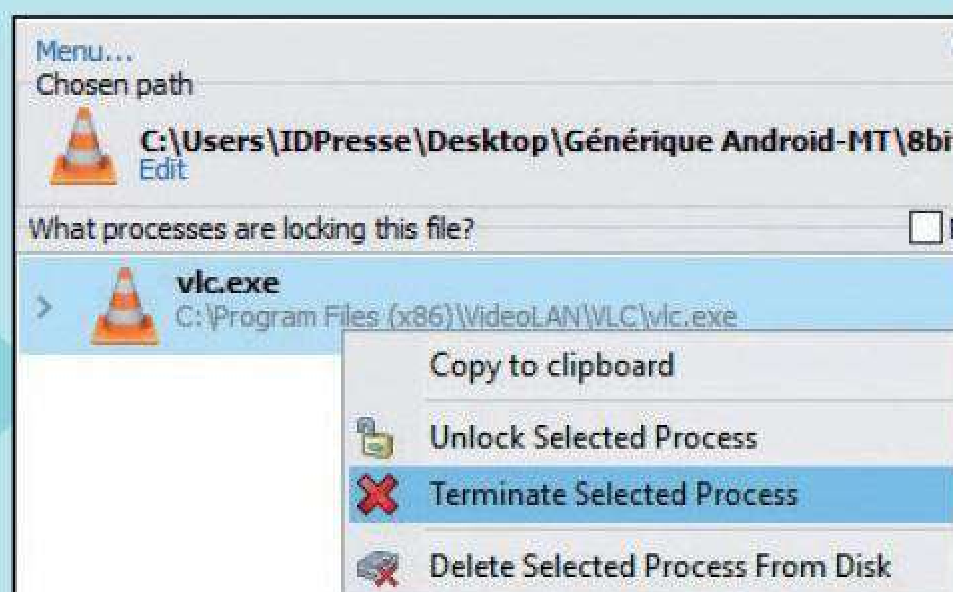




INFOS [LOCKHUNTER]
Où le trouver ? [**www.lockhunter.com**] Difficulté : ☠

TUTO





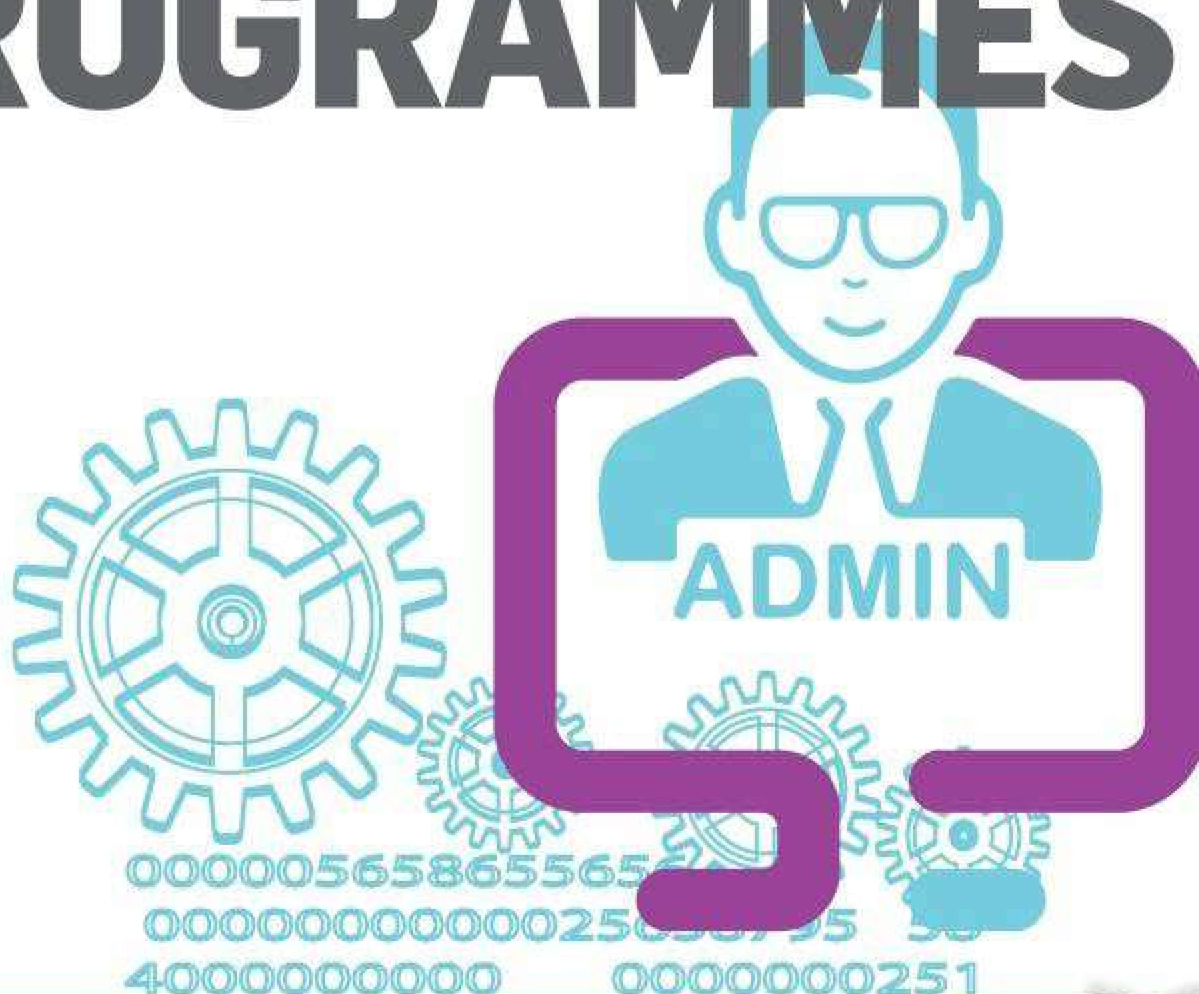
01 > TROUVER LE PROBLÈME

L'installation de LockHunter ajoute une ligne au menu contextuel. Faites un clic droit sur le fichier récalcitrant et sélectionnez **What is locking this file ?** pour ouvrir le programme et afficher le(s) processus en cause.

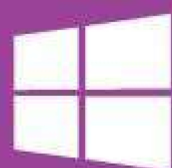
02 > TERMINER LE PROCESSUS

Faites un clic droit sur le processus puis **Terminate Selected Process**, opération qu'il faudra confirmer avec **Oui**. Vous pouvez ensuite supprimer le fichier ainsi « libéré » avec **Delete**. Il se retrouve alors dans la corbeille.

DÉBLOQUEZ LES PROGRAMMES

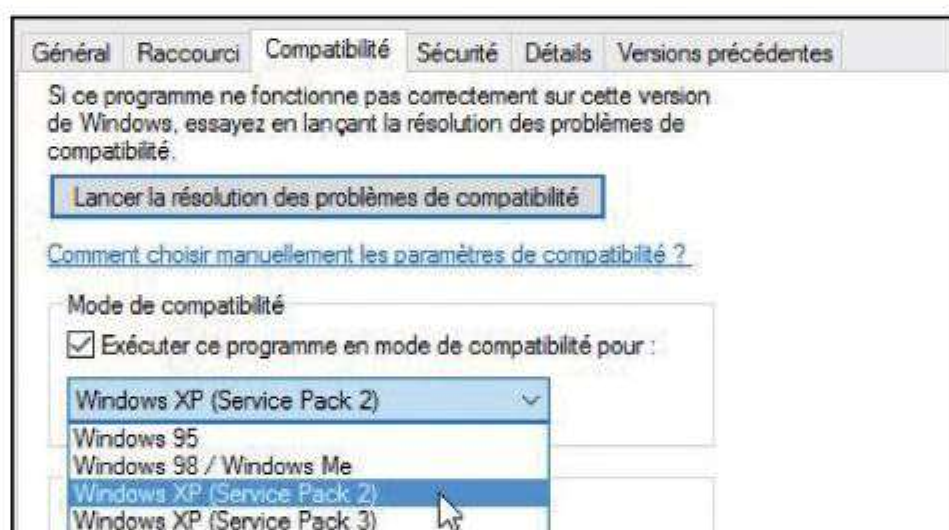


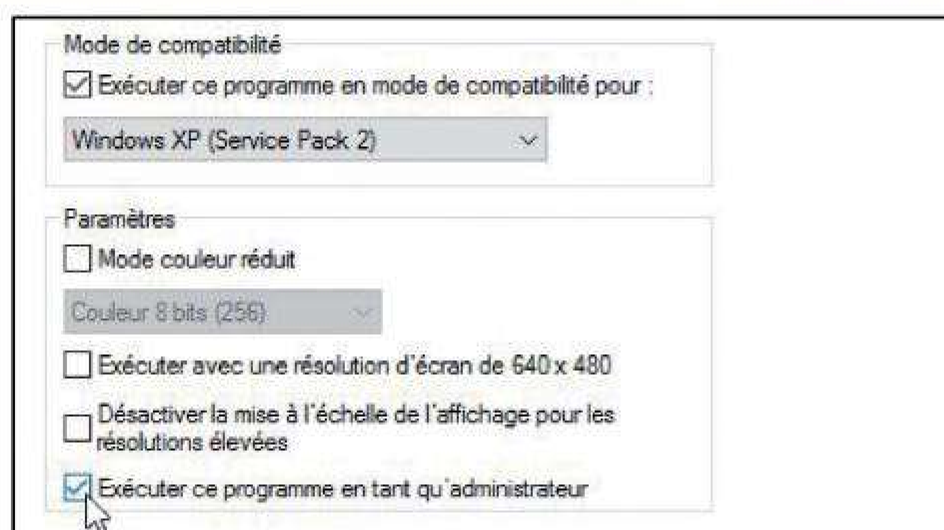
Un logiciel refuse de se lancer ? C'est peut-être qu'il n'est pas compatible avec votre version de Windows, ou exige un mode particulier.



INFOS [WINDOWS] Difficulté : ☠

TUTO





01 › EXPLOITER LE MODE DE COMPATIBILITÉ

Trouvez le dossier du logiciel (dans **C:\Programmes** ou **C:\Program Files (x86)**), faites un clic droit sur le fichier exécutable (.exe), et cliquez sur **Propriétés**. À l'onglet **Compatibilité**, cochez **Exécuter ce programme en mode de compatibilité pour** et essayez une version plus ancienne de Windows.

02 › EXÉCUTER EN TANT QU'ADMINISTRATEUR

Le mieux est de rétrograder progressivement dans la version de Windows, jusqu'à trouver celle qui convient. Si vos essais restent vains, essayez en plus de cocher la case **Exécuter ce programme en tant qu'administrateur**, en bas de la fenêtre. Avec un peu de chance...

REVENEZ EN ARRIÈRE



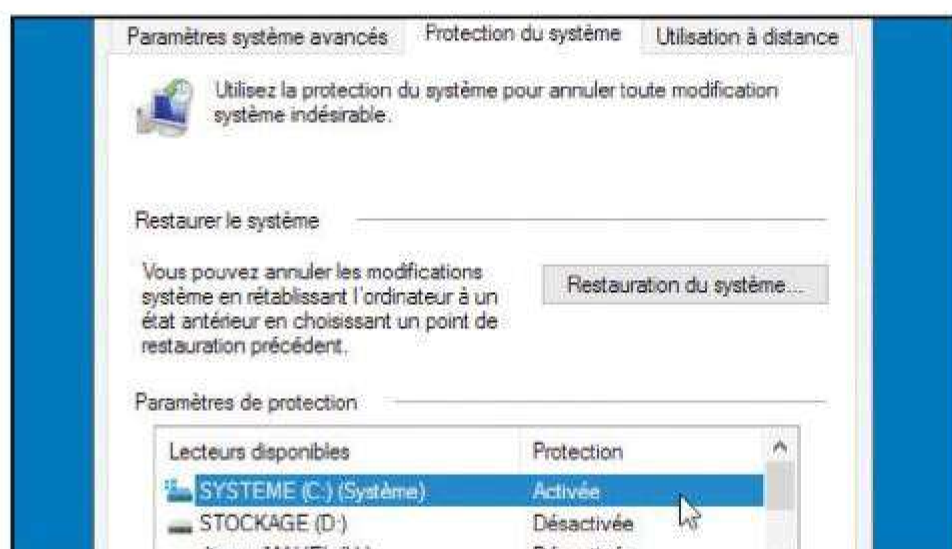
Depuis quelques jours, Windows fait des siennes ? Essayez de revenir en arrière, en restaurant le système dans l'état où il était avant que les choses tournent mal.

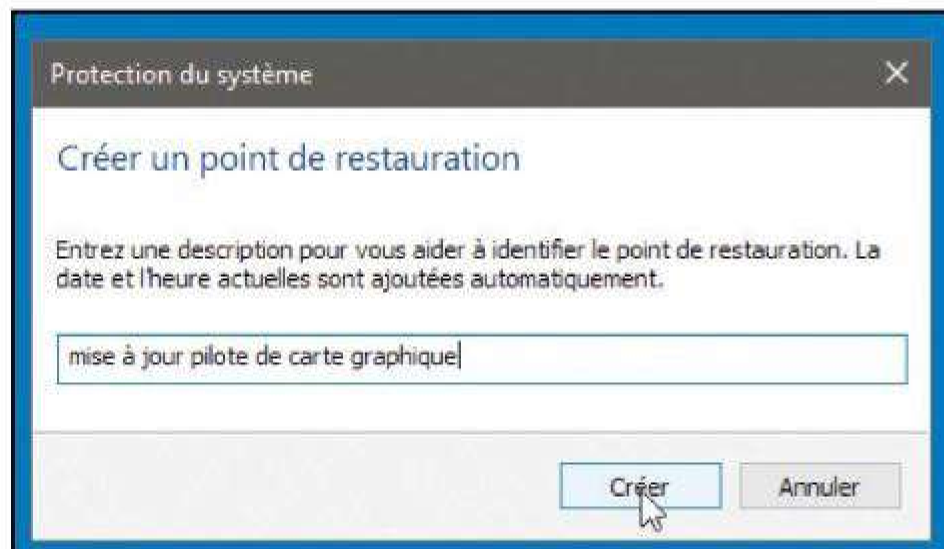
Un point de restauration, c'est un peu comme un instantané de Windows, qui vous permet de revenir en arrière, à un moment où le système était stable, si vous rencontrez des problèmes. Normalement, Windows crée automatiquement des points de restauration lors d'événements importants : mise à jour critique, installation d'un nouveau service, etc. Vous pouvez aussi créer un point de restauration de votre propre chef lors d'une manipulation pouvant comporter des risques (changement de pilote, installation d'un logiciel, etc.). La page ci-contre vous indique comment procéder, et comment utiliser les points de restauration en cas de problème. Attention, vos documents et données ne sont pas affectées, mais tous les logiciels installés postérieurement au point de restauration auquel vous revenez devront être réinstallés.



INFOS **[WINDOWS]** Difficulté : ☠☠☠

TUTO



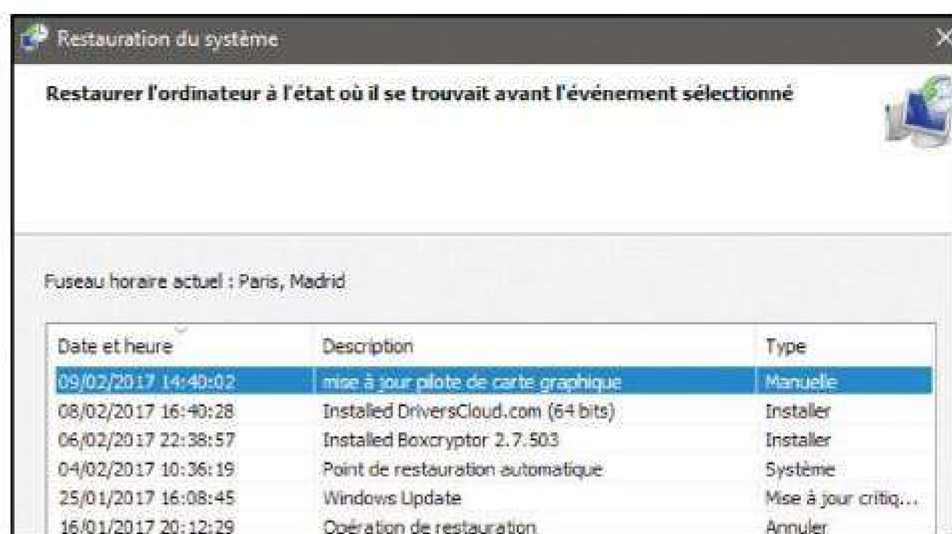


01 › ACTIVER LA PROTECTION

Tapez **restauration** dans le champ de recherche du menu Démarrer et sélectionnez **Créer un point de restauration**. Dans le cadre **Paramètres de protection**, vérifiez que la création automatique de points de restauration est bien **Activée**, au moins pour le disque système **(C:\)**. Sinon, sélectionnez cette ligne, cliquez sur **Configurer**, et activez l'option, en lui réservant au moins 5% d'espace disque. Validez par **OK**.

02 › CRÉER UN POINT DE RESTAURATION

Pour créer vous-même un point de restauration (par exemple avant de procéder à la mise à jour d'un pilote), cliquez sur le bouton **Créer**. Tapez un nom pour ce point de restauration (par exemple « mise à jour pilote de carte graphique ») puis cliquez sur **Créer**. Patientez le temps de l'enregistrement, et validez avec **Fermer**. Vous pouvez ensuite refermer la fenêtre **Propriétés système**.





03 › SÉLECTIONNER UN POINT

Pour revenir à un état antérieur de votre système, faites **Restauration du système** puis **Suivant**, et cochez la case **Afficher d'autres points de restauration**. Sélectionnez un des points et faites **Rechercher les programmes concernés** pour connaître la raison de sa création. Si vous reconnaissez l'évènement à l'origine de vos problèmes, choisissez ce point. Si vous ne savez pas quoi faire, essayez d'abord le point le plus récent.

04 › APPLIQUER LA RESTAURATION

Une fois le point de restauration choisi, sélectionnez-le et faites **Suivant**. Confirmez le disque à restaurer (a priori, C:, le disque système), faites de nouveau **Suivant**, puis **Terminer** et confirmez par **Oui**. Laissez le processus se dérouler (l'ordinateur redémarre). Si les problèmes persistent, essayez un autre point de restauration plus ancien.

DÉSINSTALLEZ UNE MISE À JOUR DE WINDOWS

Windows bénéficie de mises à jour régulières, allant du simple correctif à des évolutions plus importantes. Une de ces mises à jour cause des problèmes sur votre PC ? Voici comment la désinstaller, et éviter qu'elle soit réinstallée automatiquement.



Les mises à jour de Windows sont très importantes, car en plus d'améliorer certains aspects de votre système (performances, interface, etc.), elles colmatent des failles de sécurité critiques. Le problème c'est que ces mises à jour font parfois planter ou bugger votre système, qu'il s'agisse d'une erreur chez Microsoft ou d'un problème lié à votre PC. Le mieux est alors de supprimer la mise à jour problématique en attendant un correctif. Problème : elle risque de se réinstaller, surtout avec Windows 10, qui ne permet plus de stopper les mises à jour. L'utilitaire Win Updates Disabler permet néanmoins de bloquer ce processus.

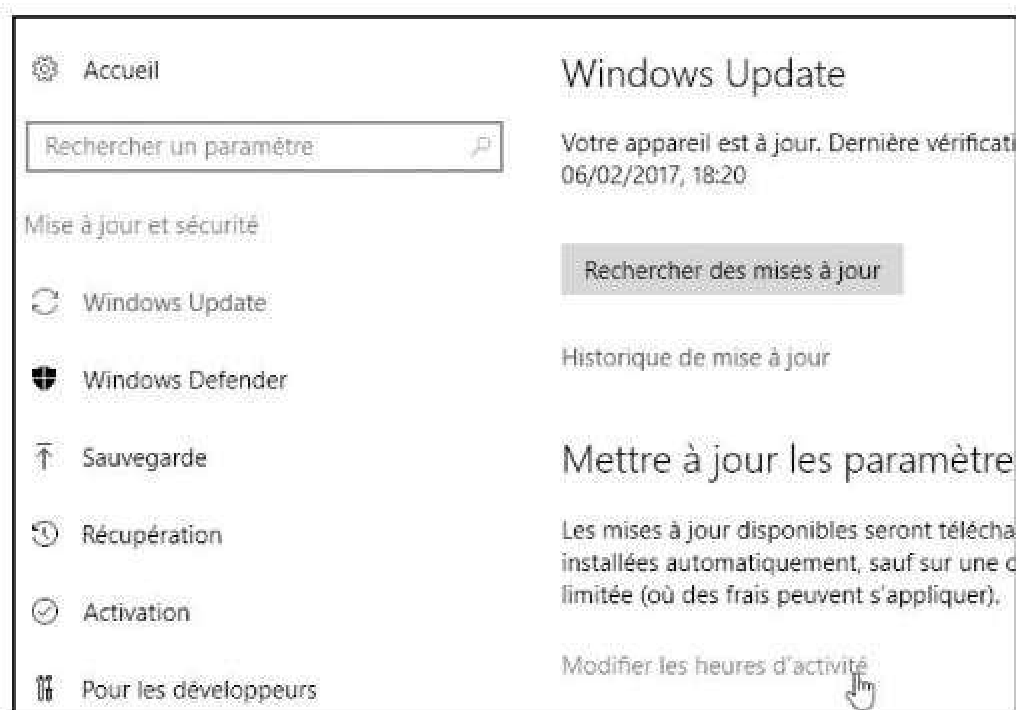
UN LOGICIEL À UTILISER AVEC INTELLIGENCE...



INFOS **[WIN UPDATES DISABLER]**

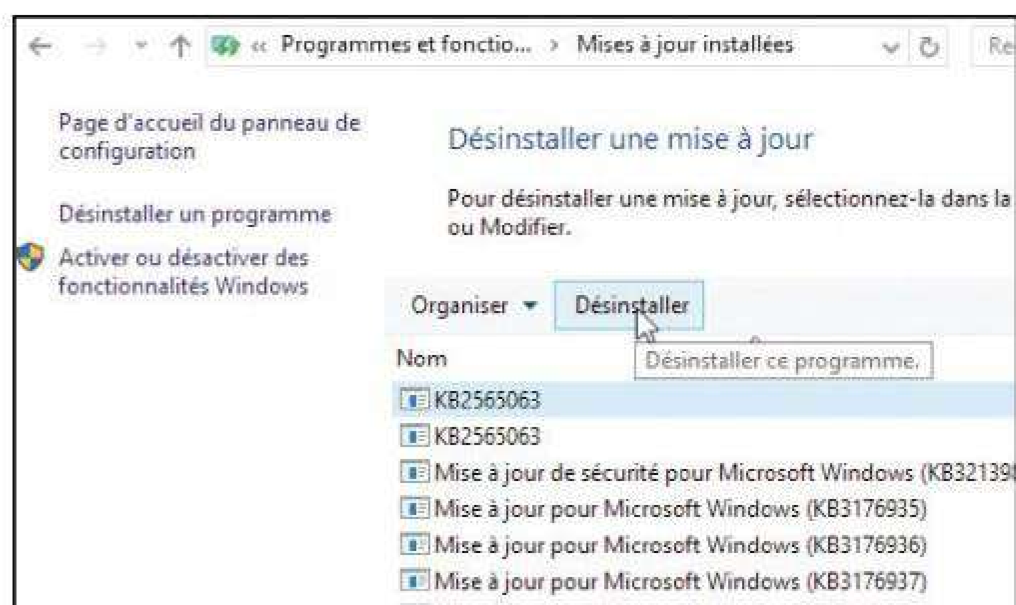
Où le trouver ? [**http://goo.gl/QGLK63**] Difficulté :

TUTO



01 › CONFIGURER WINDOWS UPDATE

Pour régler les mises à jour, avec Windows 7 allez dans le Panneau de configuration, à la section **Windows Update.** Avec Windows 10, allez dans les **Paramètres**, section **Mise à jour et sécurité**. Avec cette dernière version du système, impossible de bloquer les mises à jour automatique. Mais vous pouvez aller dans **Modifier les heures d'activité** ou **Options de redémarrage** pour éviter les redémarrages intempestifs après mise à jour pendant que vous travaillez.



02 › DÉSINSTALLER DES MISES À JOUR

Pour désinstaller une mise à jour, allez à la section **Programmes et fonctionnalités** du **Panneau de configuration** (avec Windows 10, clic droit sur le menu Démarrer). Puis cliquez sur le lien **Afficher les mises à jour installées**, à gauche. Les mises à jour de Windows sont identifiées avec le code KB. Cliquez sur la mise à jour problématique (souvent la dernière) et faites **Désinstaller**.



03 › GELER LES MISES À JOUR

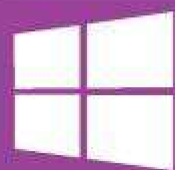
Pour éviter que Windows ne réinstalle cette mise à jour, en attendant qu'un correctif soit publié, vous pouvez utiliser Win Updates Disabler qui va simplement bloquer les mises à jour. Dans l'onglet **Désactiver**, cochez **Désactiver les mises à jour de Windows** et faites **Appliquer maintenant**. Ce tour de passe-passe fonctionne avec toutes les versions de Windows depuis XP. Attention, ne désactivez pas le Centre de sécurité, Defender ou le Pare-feu, sauf si vous savez ce que vous faites...

RÉPAREZ OU RÉINSTALLEZ WINDOWS



En cas de problème vraiment sérieux, il va falloir envisager une réparation du système, voire sa réinstallation complète. Attention, certains outils sont nécessaires pour cela, qu'il faut avoir préparés avant : faite-le dès maintenant !

Toutes les tentatives précédentes, désinstallation de mises à jour ou restauration du système, sont restés vaines ? Il faut passer à l'étape supérieure, la réparation de Windows, voire sa réinstallation dans les cas graves. Windows 7 et 10 offrent pour cela de nombreux outils. Dans les pages qui suivent, nous détaillons les méthodes à employer, de la plus douce (simple réparation) à la plus radicale (réinstallation complète). Tentez-les dans l'ordre, en sachant que dans certains cas, vous effacerez vos programmes, qu'il faudra réinstaller. Mieux vaut également effectuer une sauvegarde de tous vos fichiers. Les deux premières étapes sont consacrées à la création d'outils de réparation et de réinstallation, à entreprendre à titre préventif, avant que d'éventuels problèmes surviennent.

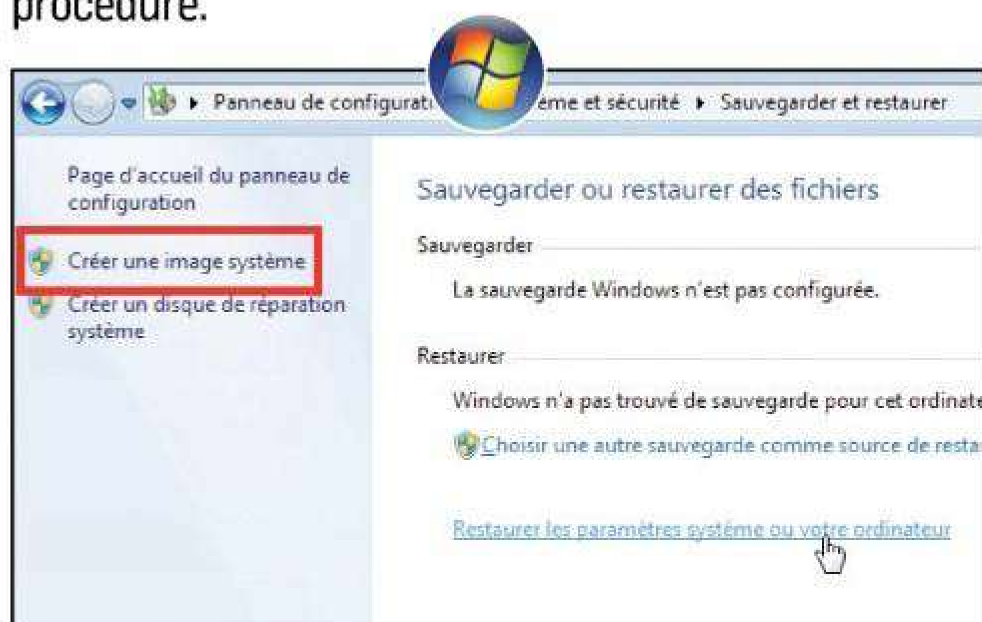


INFOS **[WINDOWS]** Difficulté : ☠☠☠

TUTO

01 › CRÉER UNE IMAGE SYSTÈME

Une image système permet de restaurer l'ordinateur dans l'état où il était lors de la création de l'image. À faire avant l'apparition de problèmes ! Munissez-vous d'un disque dur externe d'au moins 500 Go. Sous Windows 7, allez dans **Panneau de configuration > Système et sécurité > Sauvegarder et restaurer**. Sous Windows 10, allez dans **Paramètres du PC > Mise à jour et sécurité > Sauvegarde**, cliquez sur **Accéder à l'outil Sauvegarder et restaurer (Windows 7)**. Dans les deux cas, cliquez sur **Créer une image système**, à gauche, sélectionnez le bon lecteur et faites **Suivant** pour lancer la procédure.

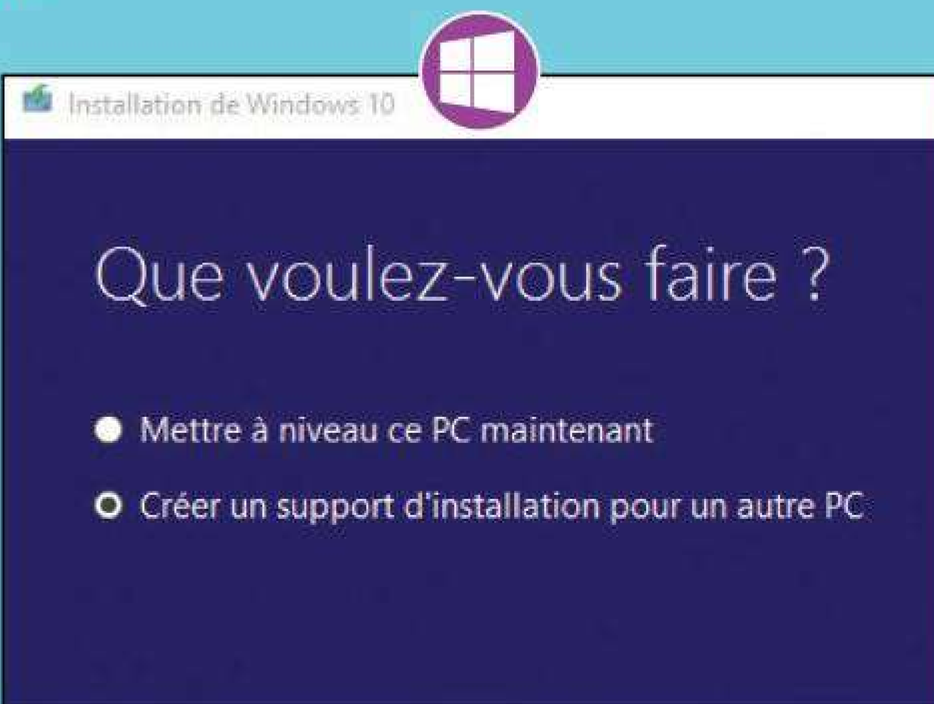




02 › CRÉER UNE CLÉ USB DE RÉPARATION

Pour réparer Windows, vous pouvez utiliser une clé USB, à préparer sur un autre PC si le vôtre ne fonctionne plus. Il faut une clé d'au moins 8 Go. Pour Windows 10, rendez-vous sur **https://goo.gl/LPwbKF** et récupérez l'utilitaire fourni par Microsoft. Lancez-le, cliquez sur **Créer un support d'installation pour un autre PC** puis **Suivant**. L'ISO de Windows sera téléchargé à la fin. Pour Windows 7, téléchargez l'ISO de votre OS à l'aide de votre clé de licence, sur le site **https://goo.gl/e1GDCM**. Utilisez ensuite le logiciel WUDT (**https://goo.gl/28R8X2**) pour finaliser la procédure.

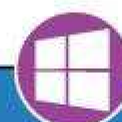




03 › ACCÉDER AUX OUTILS DE RÉPARATION DEPUIS WINDOWS

Sous Windows 10, rendez-vous dans les **Paramètres du PC > Mise à jour et sécurité > Récupération** et cliquez sur **Redémarrer maintenant**, sous **Démarrage avancé**. Vous atterrissez sur l'écran des options. Avec Windows 7, il faut redémarrer le PC et dès le redémarrage tapoter la touche **F8** (ou **F11/F12**, selon votre modèle) pour arriver sur un écran noir ou vous pourrez choisir **Réparer l'ordinateur** avec la touche **Entrée**. Le panneau des options s'ouvre alors.

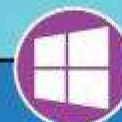




04 › TENTER UNE RÉPARATION

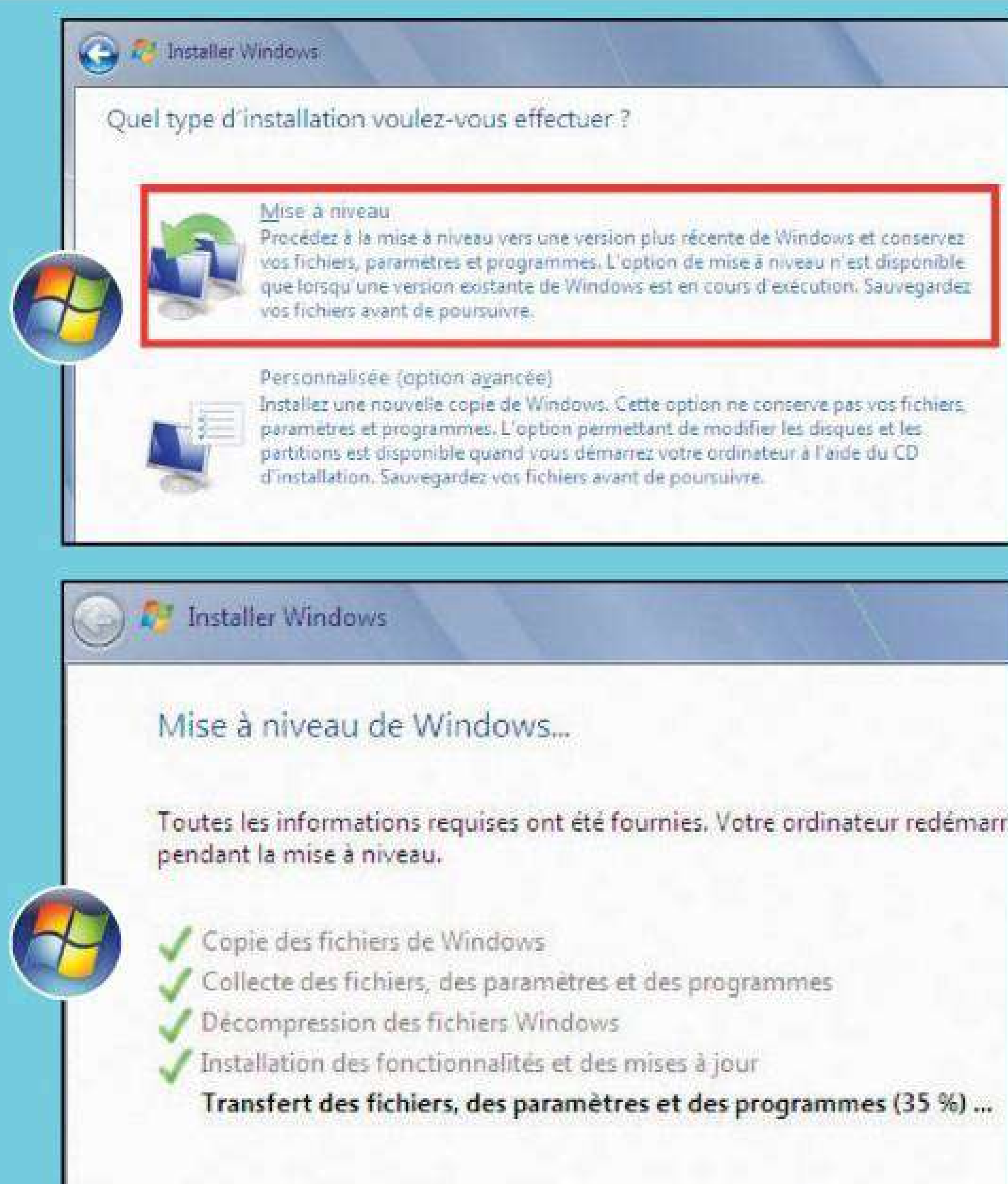
Une fois sur l'écran des options, la réparation du démarrage de Windows est la première chose à tenter, puisqu'elle ne touche pas à vos fichiers ou programmes. Sous Windows 10, cliquez sur **Dépannage > Options avancées > Outil de redémarrage système**. Il faut choisir un compte d'utilisateur et entrer son mot de passe pour lancer la réparation. Sous Windows 7, cliquez sur **Réparation du démarrage**. Après l'opération, cliquez sur **Terminer** pour redémarrer (si la réparation a réussi).





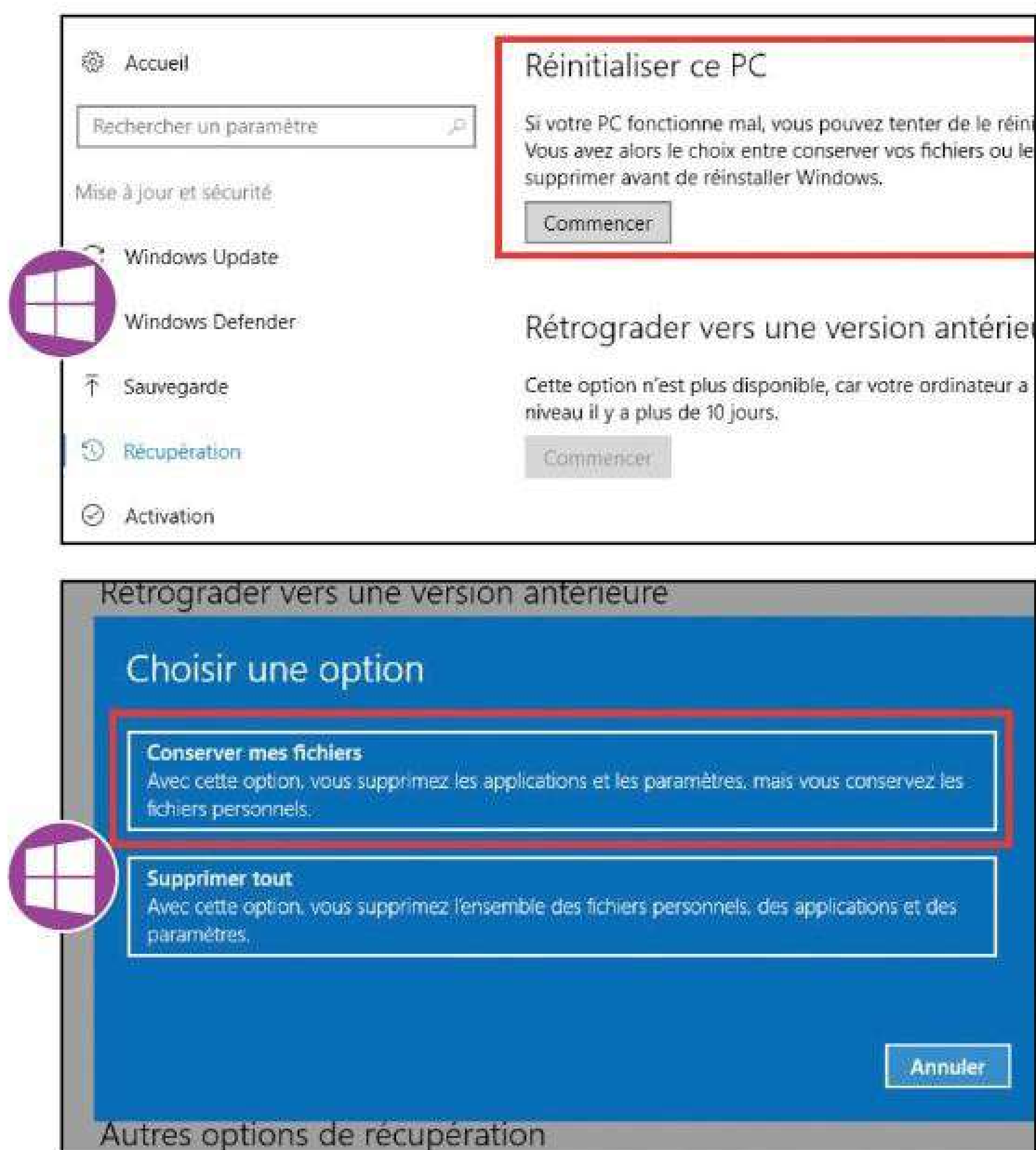
05 › RÉINSTALLER LE SYSTÈME SANS RIEN EFFACER (WINDOWS 7)

Windows 7 possède une option appelée **Mise à niveau**, qui est en fait une réinstallation de Windows sans perte de fichiers et de programmes. Il vous faut le DVD original de Windows ou une clé d'installation de Windows 7 (voir étape 2) et un accès au bureau du PC (s'il ne démarre pas, voir étape 9 et 10). Lancez le DVD ou branchez la clé et double-cliquez sur le fichier **setup.exe**. Cliquez ensuite sur **Installer maintenant**, validez le téléchargement des mises à jour puis choisissez **Mise à niveau**.



06 › RÉINSTALLER WINDOWS EN CONSERVANT SES FICHIERS (WINDOWS 10)

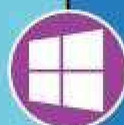
Cette option efface vos programmes et applications (il faudra les réinstaller), mais ne touche pas à vos fichiers. Allez dans les **Paramètres du PC > Mise à jour et sécurité > Récupération**. Sous **Réinitialiser ce PC**, cliquez sur **Commencer**. Cliquez ensuite sur **Conserver mes fichiers**. Suivant votre PC, une troisième option, **Restaurer les paramètres d'usine**, peut apparaître. Notez que les applications et programmes préinstallés ne seront pas supprimés.



07 › UTILISER UNE IMAGE SYSTÈME

Attention : vous retrouverez votre PC (fichiers et programmes) tel qu'il était au moment de la création de l'image. Donc l'opération peut s'avérer quelque peu destructrice si l'image est ancienne. Branchez le périphérique contenant l'image puis référez-vous à l'étape 3 pour accéder aux options de réparation. Sous Windows 10, allez dans **Dépannage > Options avancées > Récupération de l'image système**. Sous Windows 7, cliquez sur **Récupération de l'image système**. Suivez les instructions dans les deux cas.

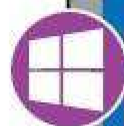




08 › RÉINSTALLER WINDOWS EN SUPPRIMANT TOUT (WINDOWS 10)

Quelquefois, même si c'est rare, un ou plusieurs fichiers peuvent être la cause de dysfonctionnements. Ou peut-être voulez-vous profiter de la réinstallation de Windows pour faire un peu de ménage. Dans les deux cas, comme à l'étape 6, allez dans les **Paramètres du PC > Mise à jour et sécurité > Récupération**. Sous **Réinitialiser ce PC**, cliquez sur **Commencer**. Choisissez cette fois-ci **Supprimer tout**. L'opération étant irréversible, assurez-vous d'avoir sauvegarder vos fichiers importants.





09 › DÉMARRER SUR UN SUPPORT EXTERNE

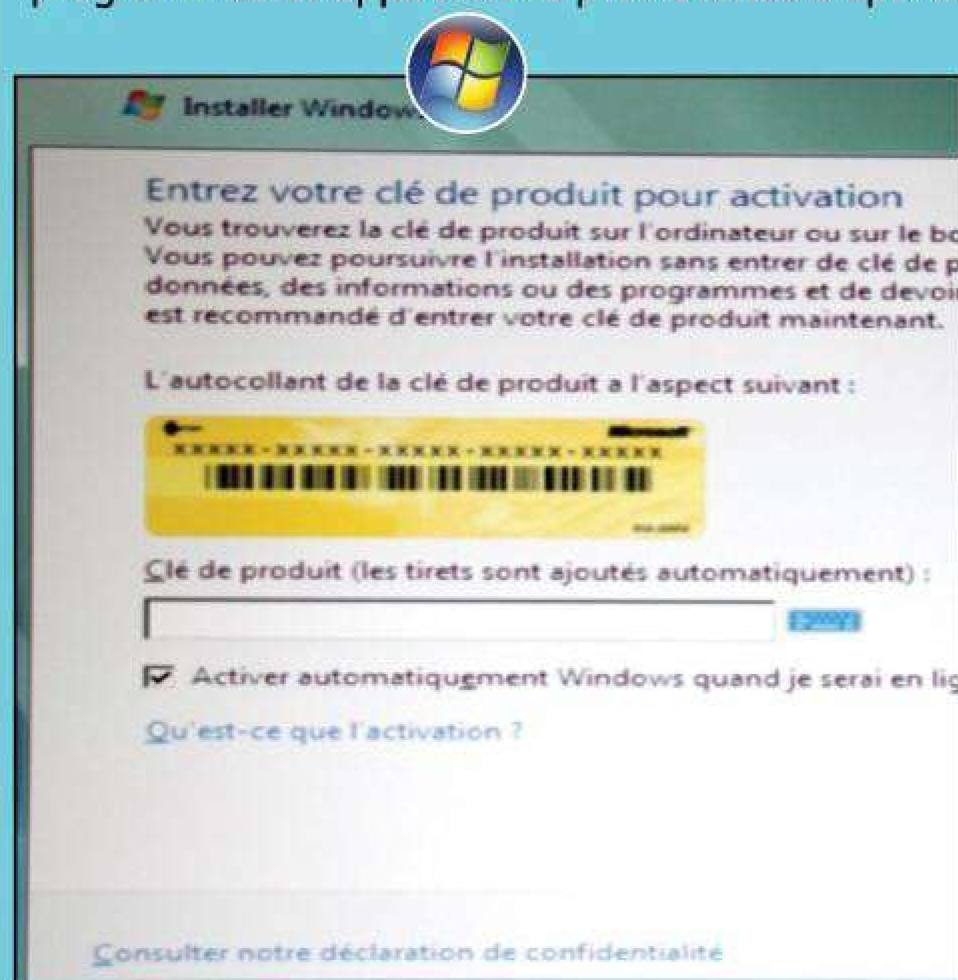
La plupart des opérations précédentes supposent que vous avez accès à votre ordinateur, et qu'il fonctionne à peu près normalement le temps d'effectuer les opérations. Si le PC ne veut plus démarrer, la seule solution est de passer par un support de réparation/réinstallation externe, tel que créé aux étapes 1 et 2. Il faut démarrer l'ordinateur sur ce support externe.

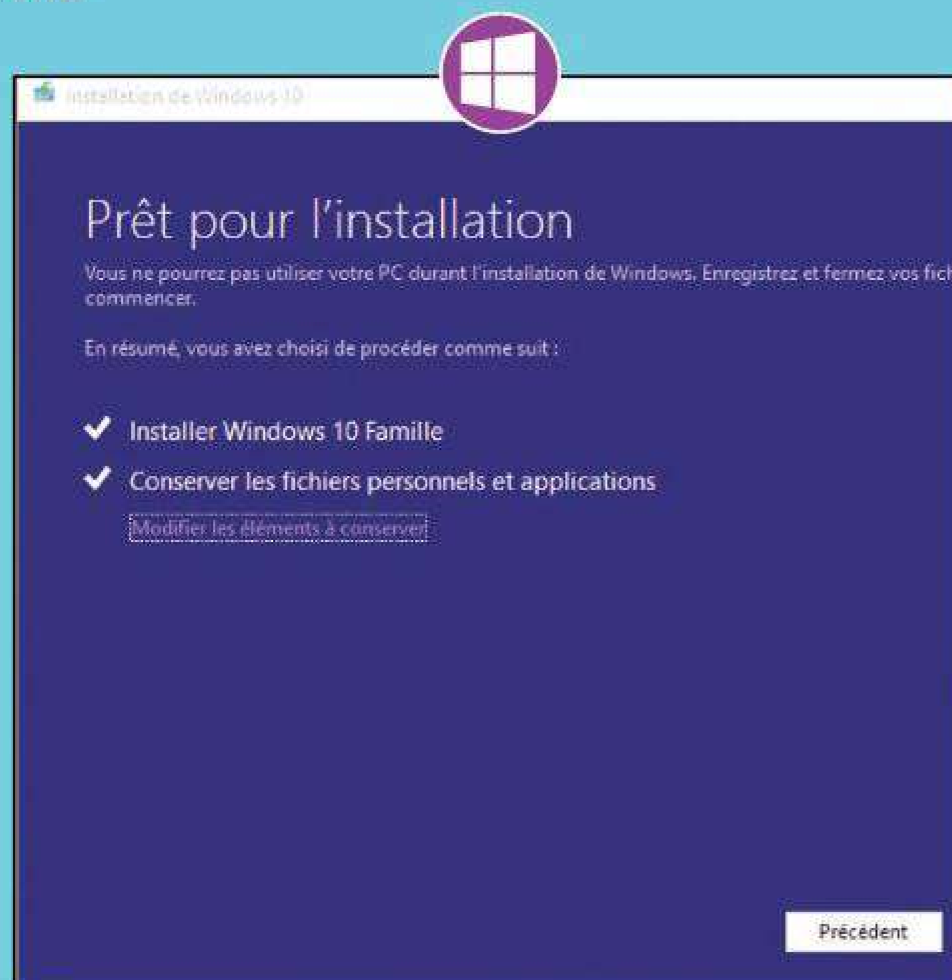




10 › RÉINSTALLER WINDOWS COMPLÈTEMENT

Une fois que vous avez redémarré sur un support externe, que ce soit un DVD d'installation ou une clé USB, vous retrouvez la même interface et les mêmes options de réparation/réinstallation qu'aux étapes précédentes. Vous n'avez plus qu'à faire votre choix et suivre les instructions affichées à l'écran. Dans le cas d'une réinstallation complète de Windows depuis un support externe, même les programmes et applications préinstallés disparaîtront.







RETROUVEZ CLÉS ET NUMÉROS DE LICENCE



Si vous devez réinstaller Windows et vos logiciels, vous allez avoir besoin de leurs clés d'activation, des numéros de licence, et d'éventuels mots de passe. Voici comment les retrouver.

Difficile de faire plus simple que recALL. Après l'avoir installé, il suffit de laisser faire le logiciel. Il va chercher des mots de passe, des codes d'accès ou des numéros de licence dans des recoins de votre système dont vous ne soupçonnez même pas l'existence (dossier d'installation, registre, dossiers cachés, etc.). Ces emplacements sont préenregistrés et toutes sortes de logiciels sont passés au crible : Windows, Office, antivirus, clients de messagerie, navigateurs Internet, clients FTP, messageries instantanées, logiciels commerciaux, jeux vidéo, code d'accès Wi-Fi, etc. Attention, recALL pouvant être dangereux s'il est placé entre de mauvaises mains (celles d'un vilain curieux), il est bloqué par Windows Defender, l'antivirus de Windows. Il faut donc désactiver ce dernier, avant de télécharger le programme.



INFOS **[RECALL]**

Où le trouver ? [**https://keit.co/p**] Difficulté : ☠☠☠

TUTO



Voici une liste de mots de passe récupérés. Si vous souhaitez les exporter, cliquez sur suivant.

Application	Ressource	Connexion	Mot de passe
{9D3D8C60-A55F-4fed-			{9D3D8C60-A55F-4fed-B2B9-1730012
Advisor			d7b60e7f
Avast 8.x			S9999999T9901A1106-U1N7ALRH
Avast 8.x			271DF1FB-E411-4EE3-9D2D-CA2AF355
Nero	Nero 10		2X24-K08K-KLU8-CU07-8E33-HP1Z-L2
Internet Explorer			00359-OEM-8992687-00017
Windows 7 Home Prem	Microsoft License		6GF36-P4HWR-BFF84-6GFC2-BWX77
Microsoft License	Microsoft License		RHPQ2-RMFJH-74XYM-BH4JX-XM76F
Microsoft Internet Expl	Microsoft License		6GF36-P4HWR-BFF84-6GFC2-BWX77

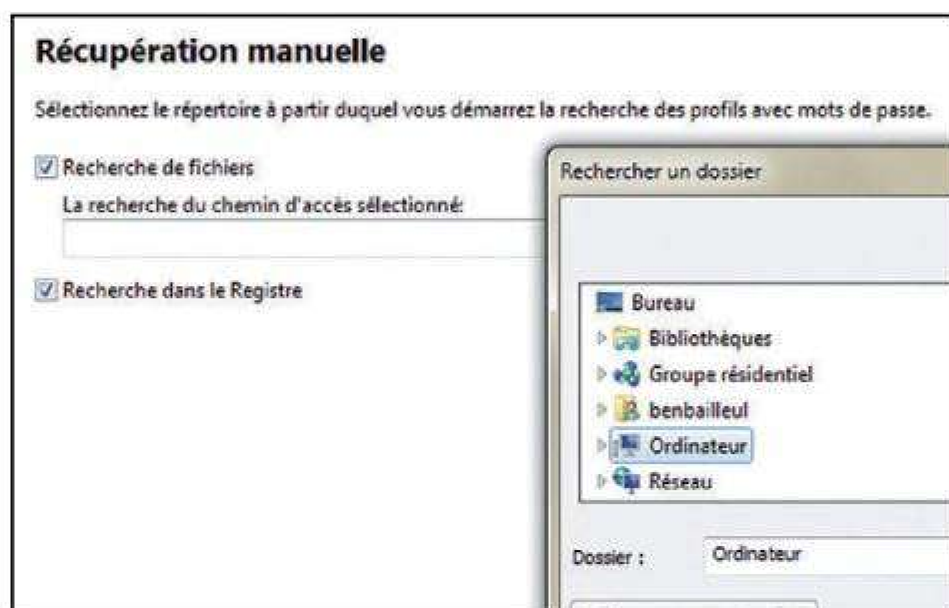
Recherche:C:\Program Files (x86)\Popcorn...\librtp_plugin.dll

01 › DÉSACTIVER WINDOWS DEFENDER

Cliquez sur l'icône de Windows Defender, dans la barre système, à l'extrémité de la barre des tâches. Allez dans **Protection contre les virus et menaces**, puis **Paramètres de protection**... et placez le curseur **Protection en temps réel** sur **Désactivé**. Vous pouvez maintenant télécharger et installer RecALL.

02 › RÉCUPÉRER LES MOTS DE PASSE

Le logiciel scanne tout votre disque dur à la recherche du moindre mot de passe. Cela peut prendre plusieurs minutes, mais au final, vous aurez absolument tous les sésames que contient votre PC, y compris les codes Wi-Fi et les clés de licence. En faisant **Suivant**, vous pouvez sauvegarder les résultats aux formats CSV, HTML, TXT, ZIP ou KeePass.



Émulation serveur

Dans la prochaine étape seront exécutés serveurs de messagerie et FTP qui permettr la récupération des mots de passe à partir de pratiquement tous les programmes qui prennent en charge ces services

1. Exécutez votre logiciel de messagerie
2. Ouvrez les propriétés du compte
3. Rappelez-vous l'adresse actuelle du serveur mail/ftp entrant
4. Remplacez-le par localhost ou 127.0.0.1 et le numéro de port correct:
   POP3 - 110
   SMTP - 25
   FTP - 21
5. Recevez du courrier ou connectez-vous au serveur de votre compte
6. Les mots de passe apparaissent à l'étape suivante
7. Restaurez les propriétés enregistrées à l'étape3

03 › PROCÉDER MANUELLEMENT

La **Récupération manuelle** est plus précise et plus rapide, mais il faut que vous sachiez où chercher. Cliquez sur l'icône de dossier, à l'extrémité de la barre de recherche, et cochez **Recherche dans le registre**. Enfi n si votre application POP, SMTP ou FTP n'est pas dans la liste de compatibilité de recALL, vous pouvez toujours émuler un serveur de ce type pour récupérer les mots de passe.

04 › ÉMULER UN SERVEUR

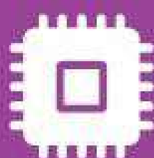
Choisissez la troisième option, faites **Autoriser** l'accès lorsque votre pare-feu se réveille, et suivez les instructions. Il faut faire pointer votre logiciel POP vers l'IP**127.0.0.1** et envoyer une requête (un message par exemple). RecALL va intercepter le mot de passe à la volée. Ici aussi, vous pourrez sauvegarder les résultats dans un fichier.

REDÉMARREZ L'ORDINATEUR AVEC UN DVD OU UNE CLÉ USB

Si Windows ne démarre même plus, il faut le DVD original ou une clé USB de secours pour relancer l'ordinateur.

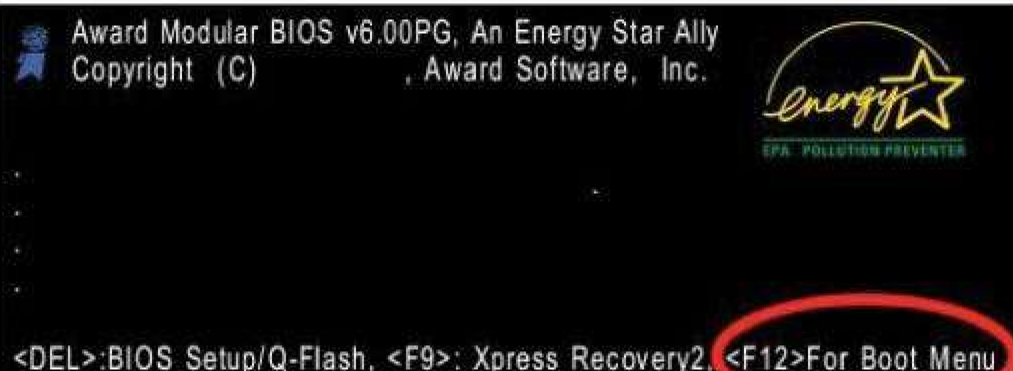
Windows ne démarre même plus à partir du disque dur, votre PC reste bloqué avant le chargement du système ? Il faut démarrer sur un DVD original de Windows, ou sur une clé USB d'installation de Windows que vous aurez créée auparavant, ou que vous réaliserez sur un autre PC. Il est possible que votre ordinateur démarre spontanément sur la clé ou le DVD lorsque vous l'allumez après avoir branché cette dernière ou inséré le disque dans le lecteur. Si ce n'est pas le cas, vous allez devoir accéder au menu de démarrage ou changer les options du BIOS, le programme de configuration lancé au tout début du démarrage.

POUR RÉINSTALLER WINDOWS, IL FAUDRA PASSER PAR LE BIOS...



INFOS [BIOS] Difficulté :

TUTO



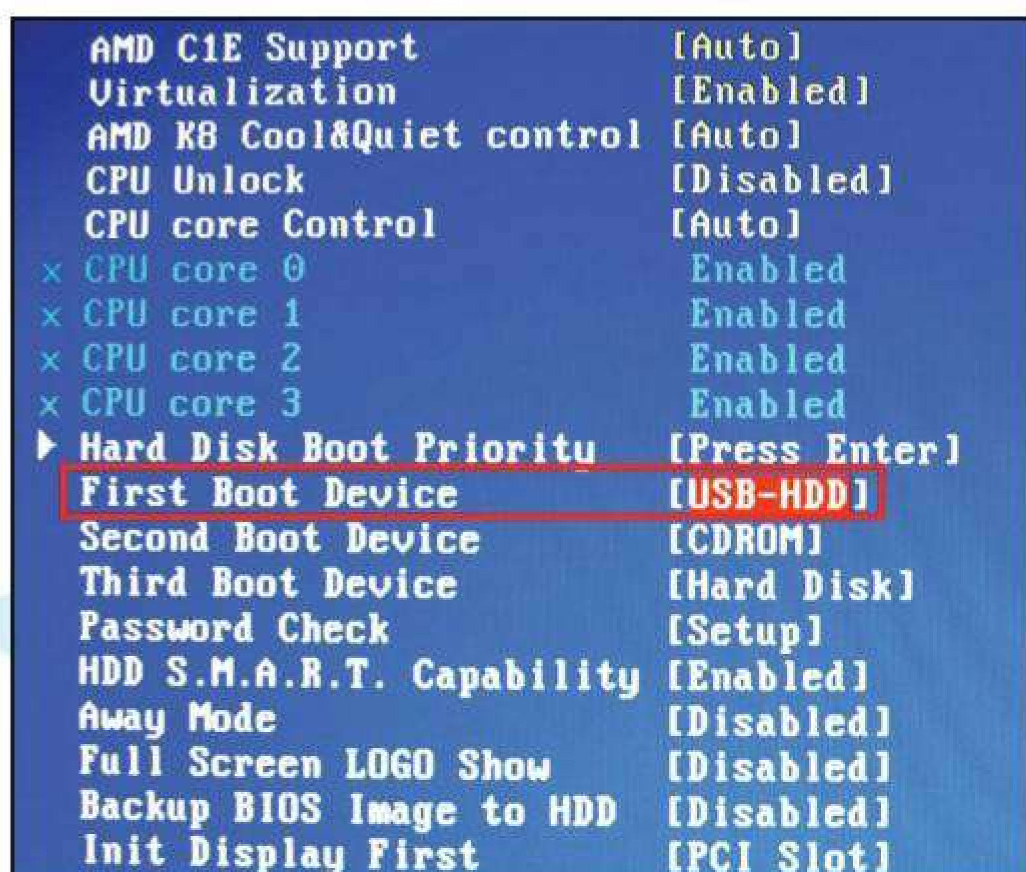
01 › OUVRIR LE MENU DE DÉMARRAGE

Démarrez le PC en tapotant sur la touche permettant d'accéder au **BOOT Menu**. Il s'agit souvent de **F12**. Parfois, la touche à utiliser s'affiche à l'écran lors du démarrage, comme ci-contre. Sinon, cherchez dans la documentation de votre ordinateur ou sur Internet.



02 › DÉMARRER SUR LA CLÉ OU LE DVD

Une liste de périphériques s'affiche. Avec les flèches du clavier, sélectionnez le disque (**CDROM**) ou votre clé USB. Cette dernière apparaît sous son nom si vous lui en avez donné un, sinon essayez l'une des lignes comprenant la mention **USB** (essayez dans l'ordre d'apparition). Validez par **Entrée**.



03 › PASSER PAR LE BIOS

Vous pouvez aussi modifier l'ordre de démarrage dans le BIOS. Ouvrez ce dernier en frappant la touche **Suppr** au démarrage de l'ordinateur (ou autre touche le cas échéant). Sélectionnez **Advanced Bios Features**, descendez jusqu'à **First Boot Device** et appuyez sur **Entrée**. Choisissez la ligne adéquate (CD-Rom ou USB) et validez avec **Entrée**. Puis faites **Échap > Save & Exit Setup (ici F10) > Y > Entrée**.



01# Arrêter un programme bloqué

→ Avec le Gestionnaire des tâches



Un programme reste bloqué, sans que vous puissiez le fermer ? Pour forcer l'arrêt, faites **Ctrl + Maj + Échap** pour ouvrir le **Gestionnaire des tâches**. Sélectionnez le programme en question (à l'onglet **Applications** si vous êtes sous Windows 7, à l'onglet **Processus** si vous êtes sous Windows 10 en mode **Plus de détails**), puis cliquez sur **Fin de tâche** en bas. Si une fenêtre apparait pour vous demander confirmation, cliquez de nouveau sur **Fin de tâche**.

Difficulté :

02# Éviter les redémarrages intempestifs

→ Avec Windows Update

Heures d'activité

Les heures d'activité nous permettent de savoir quand vous utilisez généralement cet appareil. Lorsqu'un redémarrage est nécessaire pour terminer l'installation d'une mise à jour, nous ne redémarrons pas automatiquement votre appareil pendant les heures d'activité.

Remarque : nous allons vérifier si vous utilisez cet appareil avant de tenter de le redémarrer.

Heure de début
8 | 00

Heure de fin
17 | 00

Enregistrer | Annuler

Pour éviter un redémarrage de Windows, après application d'une mise à jour, pendant que vous êtes en train de travailler sur l'ordinateur, vous pouvez définir des heures d'activité. Windows ne tentera pas de redémarrer pendant ces plages horaires. Ouvrez les **Paramètres** puis la rubrique **Mise à jour et sécurité**. Cliquez sur **Modifier les heures d'activité**. Sélectionnez les heures de début et de fin d'utilisation de votre PC et validez avec **Enregistrer**.

Difficulté :

03# Vérifier la version de Windows

→ Avec Windows

Windows bénéficie de mises à jour régulières, dont certaines, considérées comme majeures, sont signalées par un nouveau numéro de version. Comment savoir quelle version est actuellement installée sur votre PC ? Utilisez le raccourci clavier **Windows + R** pour ouvrir la commande **Exécuter**. Tapez **winver** et validez avec **OK**.

Difficulté :

04# Afficher les fichiers système


→ Avec l'Explorateur de fichiers

Pour éviter toute mauvaise manipulation, Windows cache les dossiers et fichiers système. Si vous souhaitez les afficher malgré tout, ouvrez l'Explorateur de fichier. Avec Windows 7, allez dans le menu **Organiser** et choisissez **Options des dossiers**... Avec Windows 10, cliquez sur l'onglet **Affichage** puis sur le bouton **Options**. à l'onglet **Affichage**, sélectionnez l'option **Afficher les fichiers, dossiers et lecteurs cachés**. Décochez ensuite la case **Masquer les fichiers protégés du système d'exploitation**. Cliquez sur **Oui** et validez avec **OK**.

Difficulté :

05# Effectuer un redémarrage d'urgence


→ Avec Windows

Vos programmes ne répondent plus, Windows se bloque ? Plutôt que d'utiliser le bouton reset ou de débrancher l'ordinateur, faites un redémarrage d'urgence. Appuyez sur **Ctrl + Alt + Suppr**. Sur l'écran qui apparaît, maintenez la touche **Ctrl** enfoncée et cliquez sur le bouton de démarrage en bas à droite. Confirmer le redémarrage avec **OK**.

Difficulté :





06# Démarrer en mode sans échec

→ AVEC WINDOWS

Le mode sans échec de Windows ne charge que les composants essentiels au fonctionnement du système. à essayer lorsque vous rencontrez un problème sérieux, comme un blocage pur et simple de Windows. Avec Windows 7, il suffit de frapper la touche **F8** au bon moment (tapotez-la régulièrement) au début du démarrage de Windows. Avec Windows 10, maintenez la touche **Maj** enfoncée et redémarrez le PC (via le menu Démarrer). Ensuite, cliquez sur **Dépannage > Options avancées > Paramètres > Redémarrer,** puis **F4, F5** ou **F6**, suivant le mode sans échec que vous souhaitez activer.



Difficulté : ☠☠☠

07# Savoir si l'on dispose d'un système 32 ou 64 bits

→ AVEC WINDOWS

Certains programmes sont proposés en version 32 bits ou 64 bits, et il faut savoir de quel type est votre système pour choisir la version adéquate. Avec Windows 10, ouvrez les **Paramètres** pour choisir **Système**. Allez ensuite dans **Informations système** puis relevez l'information mentionnée à la ligne **Type du système**. Avec Windows 7, faites un droit sur l'icône **Ordinateur** et choisissez **Propriétés**.

Difficulté : ☠☠☠

DÉSINFECTER



p56
Les différents types de **MALWARES**

p59
AVIRA : le millésime 2019

p66
WINJA, le partenaire de votre antivirus

p71
MEDICAT : la **TROUSSE À OUTILS** universelle

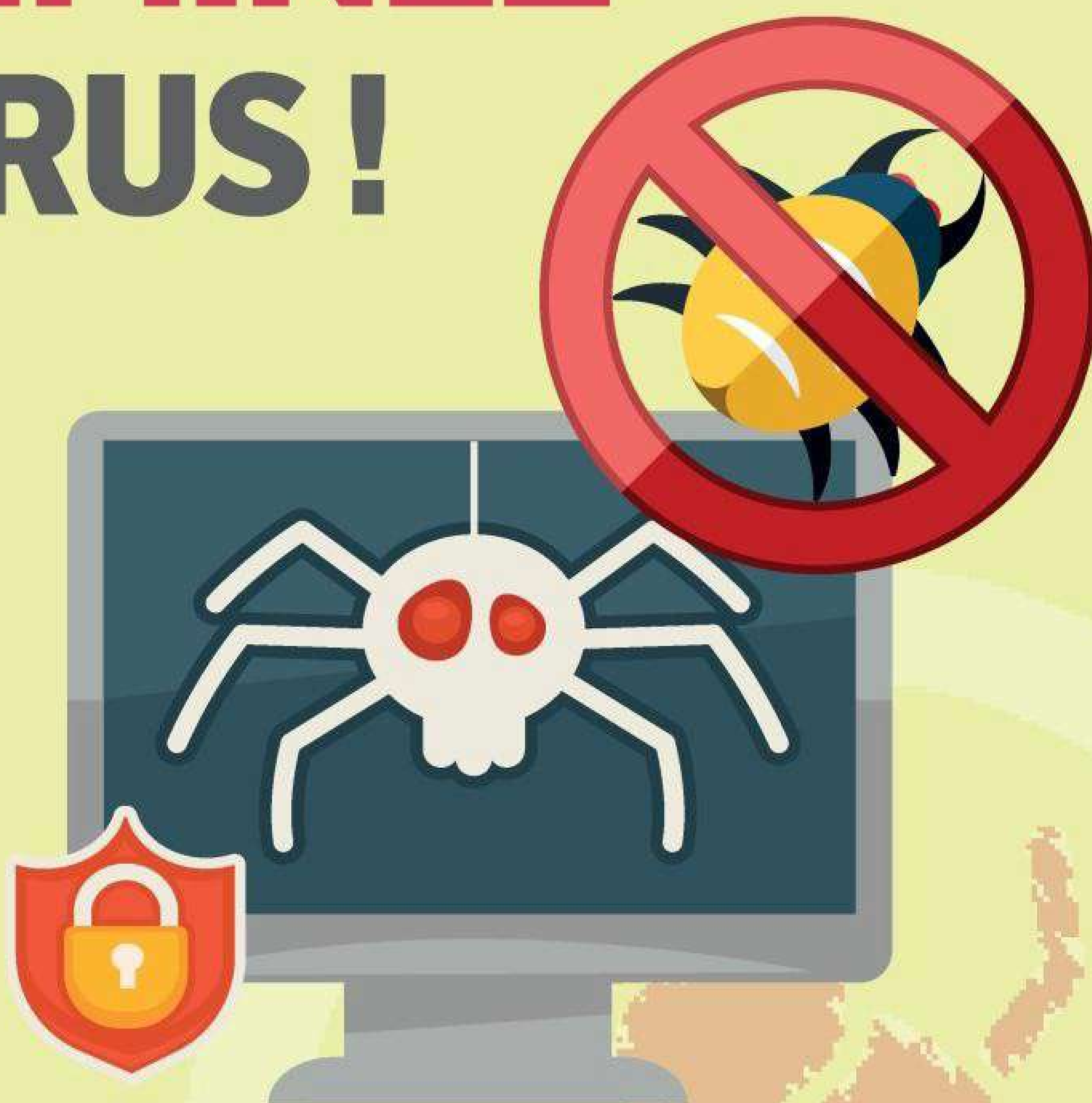
p75
Protégez-vous des **RANSOMWARES** !

p78
MICROFICHES



DÉTECTEZ ET ÉLIMINEZ LES VIRUS !

Ralentissements suspects, fenêtres surgissant pour afficher des publicités ou de faux messages d'alerte, crash à répétition... Votre PC est peut-être infecté par un virus !



Les symptômes d'une infection sont aussi variés que la nature des malwares (« logiciels malfaisants ») susceptibles de s'introduire sur votre PC, via votre connexion Internet, ou une clé USB elle-même infectée. Cela va de la simple gêne à la destruction de données, en passant par le blocage du PC. La première ligne de défense contre les virus informatiques, c'est vous. Évitez les sites louches, n'ouvrez pas les pièces jointes à des mails d'origine suspecte. La seconde barrière, c'est la protection en temps réel exercée par votre antivirus. Une protection indispensable, mais pas infaillible : un virus peut à l'occasion se glisser entre les mailles du filet. Les pages qui suivent vous expliquent comment analyser votre système en profondeur pour détecter une attaque et la neutraliser, avec votre antivirus d'abord, des utilitaires spécialisés ensuite, voire un CD de secours si Windows ne démarre même plus.

LES DIFFÉRENTS TYPES DE MALWARES



Virus : le virus « classique », aujourd'hui peu répandu, est un morceau de code malveillant qui se greffe sur un programme légitime pour faciliter sa propagation.



Ver : comme un virus sauf que celui-ci n'a pas besoin de programme hôte. il utilise des failles de sécurité pour s'introduire sur un système et se propager vers d'autres ordinateurs.



Rogueware : assez retors, il s'agit d'un faux antivirus qui va afficher des messages d'alerte bidon pour vous soutirer de l'argent.



Trojan (cheval de Troie) : il ne cause pas de tort par lui-même, mais s'invite sur une machine pour y lancer d'autres programmes malveillants ou laisser des failles de sécurité béantes.



Ransomware : très en vogue actuellement, ce type de malware interdit l'accès aux fichiers de l'utilisateur, en général en les cryptant. Pour récupérer ses fichiers… il faut payer !



Spyware : il s'agit d'un logiciel espion qui transmet vos données personnelles, et n'est pas forcément considéré comme un malware par les antivirus.



Adware : celui-ci vous affiche de la publicité dans des fenêtres de Windows ou dans votre navigateur. Comme le spyware, il faut le plus souvent un programme spécialisé pour s'en débarrasser.



Keylogger : c'est un malware qui va enregistrer vos frappes au clavier pour vous espionner ou vous voler vos mots de passe.



Rootkit : il se dissimule au sein du système en utilisant des techniques complexes pour ensuite donner des droits d'accès à un pirate ou à un autre malware.

REVENIR À UN POINT DE RESTAURATION ?

Utiliser un point de restauration Windows peut sembler une bonne idée pour revenir à une situation où le système n'était pas contaminé. Mais avec certains malwares, trop complexes et bien ancrés dans le système, la manœuvre ne fonctionne pas. Rien ne vous empêche d'essayer si les outils de décontamination ne fonctionnent pas, mais utilisez d'abord ces derniers.

CHEZ VOTRE MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

WI-FI,
ANONYME,
MOBILES,
HACKING,
ENCODAGE,
ANTIVOL,
CRYPTAGE,
MOTS DE PASSE,
SURVEILLANCE

NOUVELLE FORMULE + DE PAGES + DE HACKS + DE TUTOS

N°40



PIRATE INFORMATIQUE

Fév. / Avril 2019

NUMÉRO SPÉCIAL

ANNIVERSAIRE 10 ANS

TOP 8 HACKING
SPÉCIAL TECHNIQUES D'ATTAQUES

CRACKER LES CARTES DE TRANSPORTS ?
LES PIRATES S'ABONNENT !

COMMENT PIRATER SKYPE
EN MOINS DE 2 MINUTES ?

PÊCHE AUX GILETS JAUNES
LE PARTI PIRATE LEUR TEND LE CROCHET

Le GUIDE du HACKER

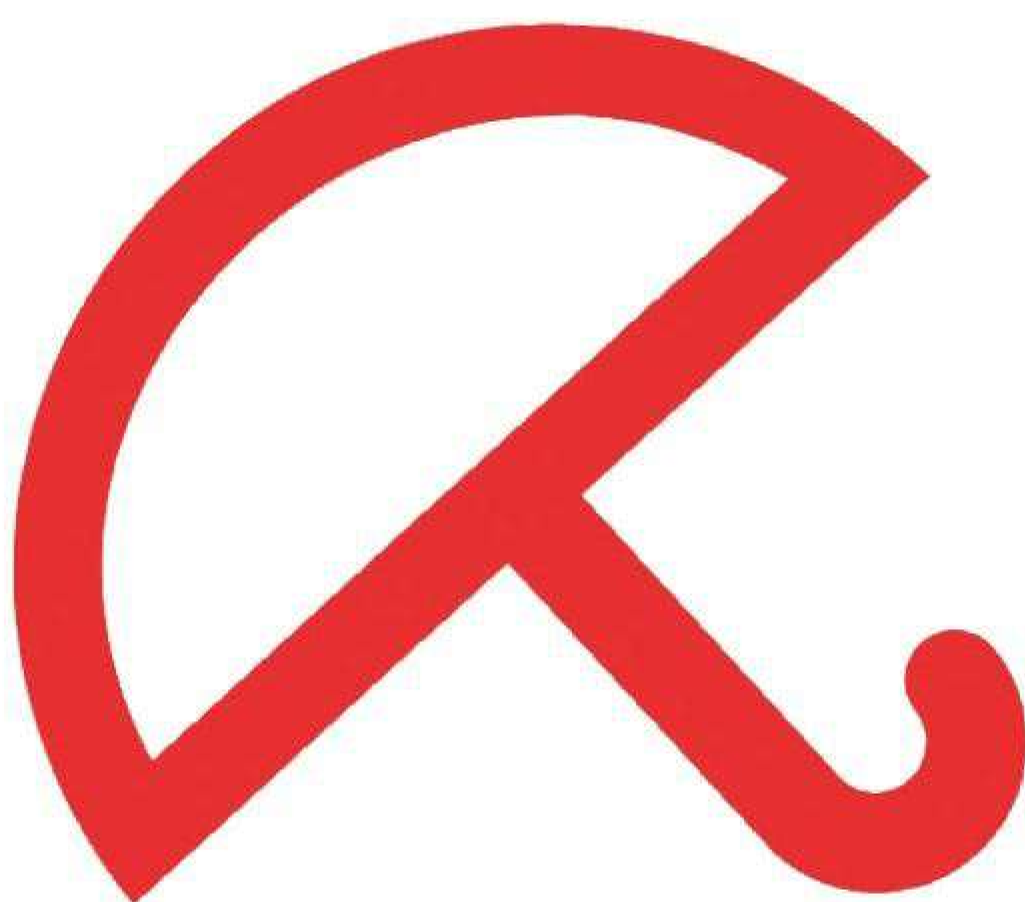
BLACK DOSSIER // Ne soyez plus esclave
Virez-moi GOOGLE par dessus-bord !
TOP 22 DES SERVICES ALTERNATIFS
AU REVOIR !

DÉCOUVREZ LES POUVOIRS DE WINJA
LA PROTECTION NOUVELLE GÉNÉRATION



NOUVELLE FORMULE
68 PAGES !

AVIRA : LE MILLÉSIME 2019



En France, l'antivirus Avast a séduit plus de 57 % des utilisateurs. Un chiffre énorme qui laisse pourtant de la marge aux concurrents. Dans ce numéro, nous allons donc vous parler de Avira Free Antivirus et de sa version payante aux nombreux modules que nous avons pu tester...



Vous voulez passer à un antivirus gratuit, car votre licence Norton ou McAfee arrive à son terme ? Comme vous avez raison ! Pour une utilisation non professionnelle, ce type de logiciel n'a plus rien à envier aux usines à gaz qui sévissaient sur nos PC dans les années 90. Doté d'un module de scan puissant, d'une protection en temps réel et de deux types de détection (une basée sur les signatures de virus et une, heuristique, basée sur le comportement d'un



malware potentiel), Avira Free Antivirus propose le kit essentiel de survie en terrain hostile.

SCAN RAPIDE ET MISES À JOUR FRÉQUENTES

Avira dispose de bons atouts comme un paramétrage très poussé : choix d'une sélection intelligente de fichiers lors du scan, octroi de plus de ressource lors d'une recherche, réglage du niveau de sensibilité de la recherche heuristique, paramétrage d'exception, etc. Les débutants laisseront tous ces réglages par défaut tandis que les plus exigeants s'amuseront à régler le logiciel pour optimiser leur protection. Au niveau de l'efficacité, il est bien difficile de se prononcer en faveur d'Avira ou d'un autre, mais grâce à sa sélection intelligente des fichiers potentiellement infectés, les scans ont été plus rapides sur nos machines de test. Notons qu'il est un des rares antivirus à avoir 3 fois la note maximale de 6 pour le site indépendant AV-Test : https://tinyurl.com/y9tlu8ak. Avoir la possibilité de télécharger des mises à jour toutes les 6 heures est aussi un plus indéniable en cas de propagation rapide d'un malware inconnu.

3 VERSIONS PAYANTES

Entre Avira Antivirus Pro 2019 (34,95€ pour un an), Avira Internet Security Suite (44,95€) et Aira Prime (99,95 €) les différences se font, bien sûr, au niveau des options. Si vous optez pour la version la moins chère, vous raterez le système de sauvegarde, le contrôle parental, les filtres antibot et antispam ou le coffre-fort à mots de passe. La version la plus chère intègre un suivi VIP, un VPN, Avira System Speedup (un outil d'optimisation des performances PC), etc. Vous trouverez un comparatif détaillé ici : **https://www.avira.com/fr/buy-antivirus.**



AVIRA ANTIVIRUS PRO 2019

Avira nous a donné l'opportunité de tester la version la plus complète de leur antivirus payant: Avira Antivirus Pro 2019.
Ce dernier ajoute son lot de modules complémentaires pour parfaire votre protection. On a un pare-feu très convivial, une surveillance des URL visitées, une surveillance des comptes e-mail POP et IMAP et la «Protection Cloud Plus» dont la seule innovation reste la mutualisation des données concernant les infections et un module permettant de scanner les dossiers partagés de type Dropbox. Cet opus 2019 intègre aussi une détection active des ransomwares, ce logiciel malveillant qui chiffre vos données personnellespour ne vous les rendre (ou pas!) que contre une grosse somme d'argent.





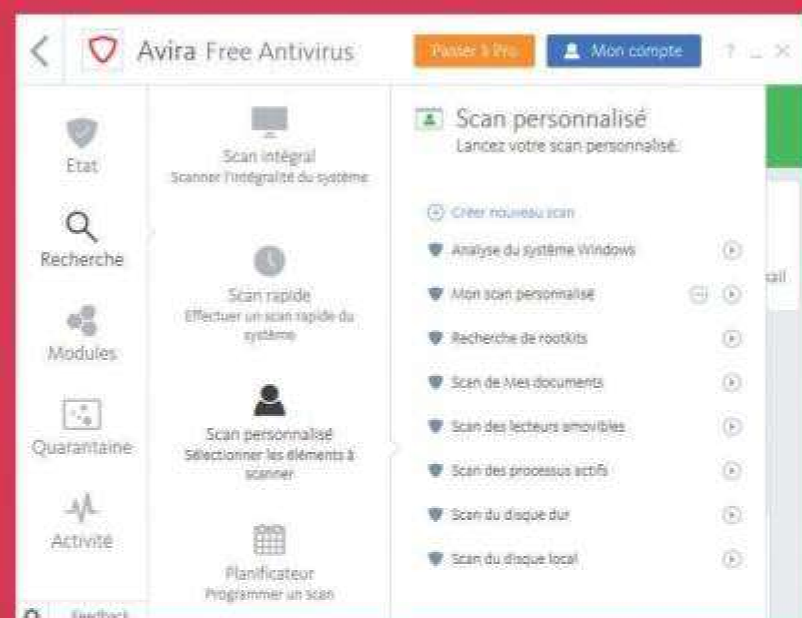
INFOS [AVIRA FREE ANTIVIRUS & AVIRA ANTIVIRUS PRO 2019]

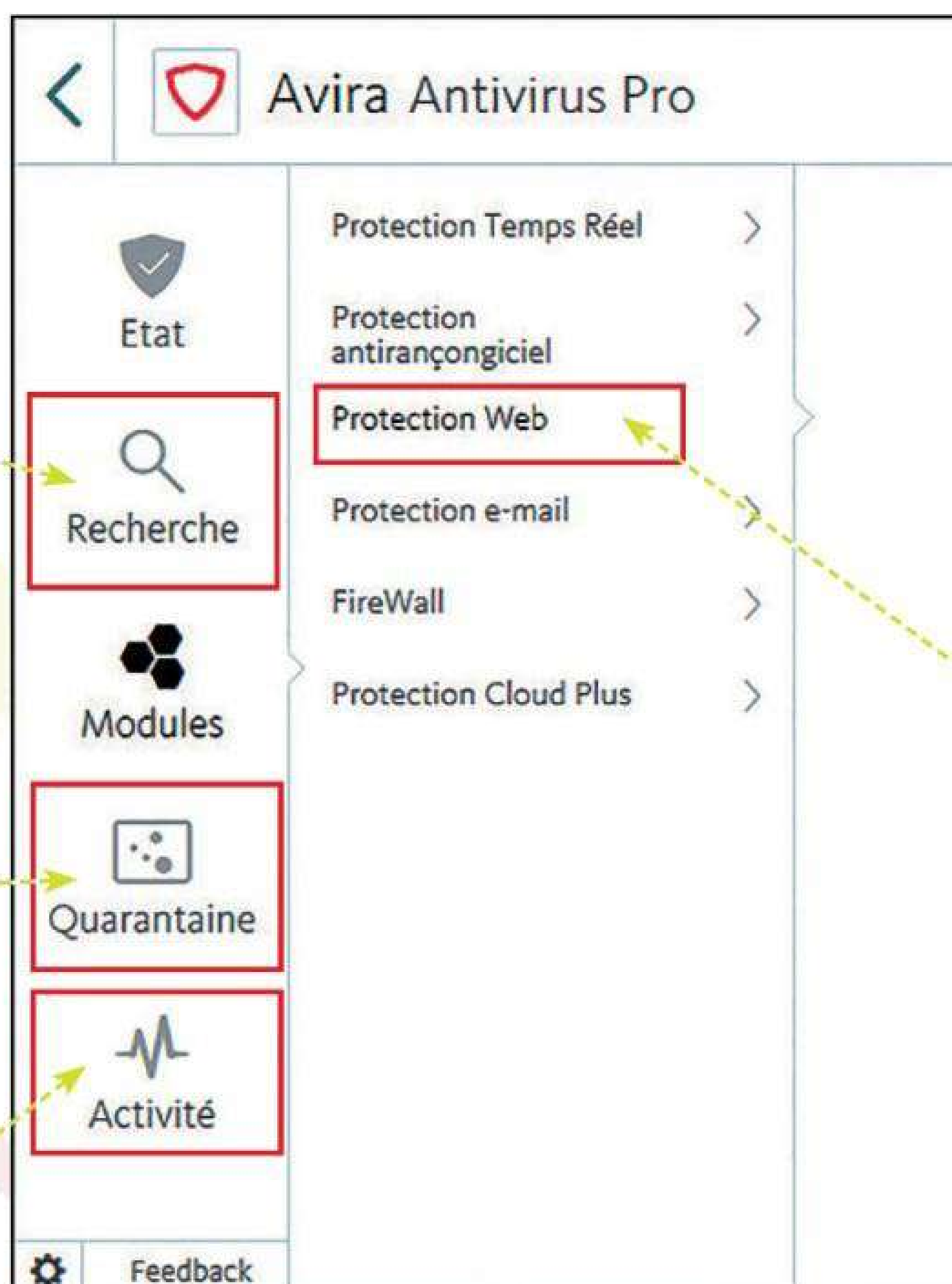
Où le trouver ? [**www.avira.com/fr**] Difficulté :

TUTO

Avast l'interface

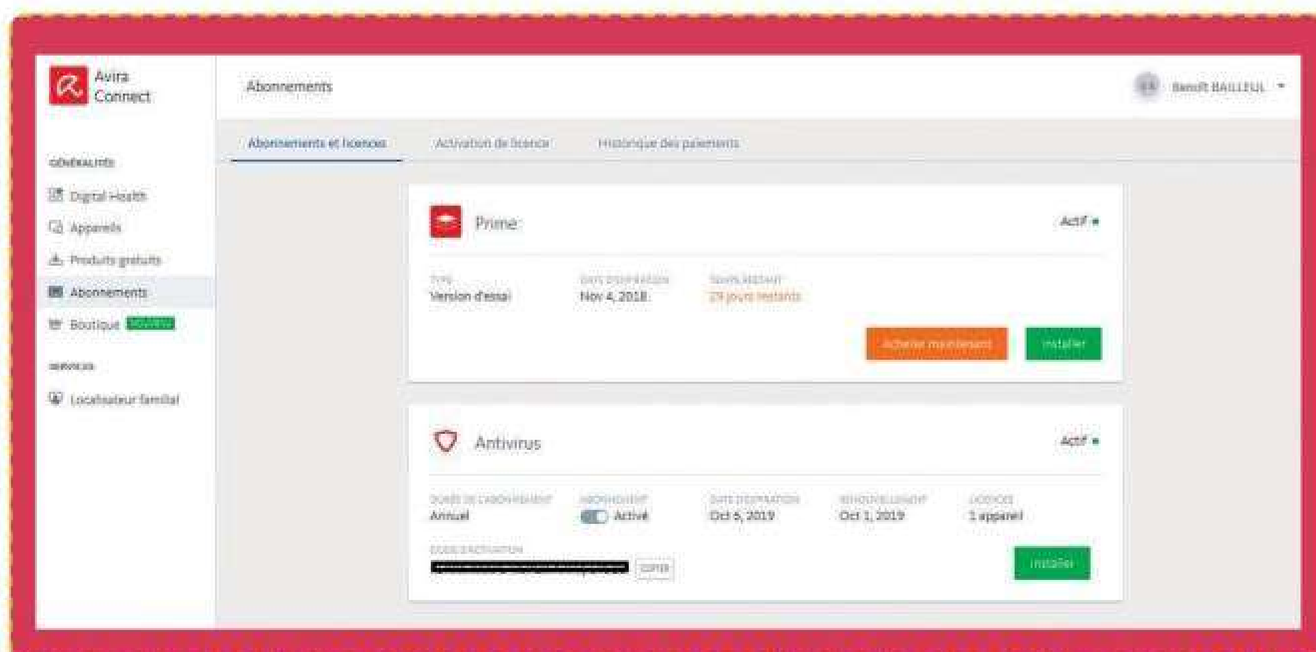
Les différents types de scans proposés



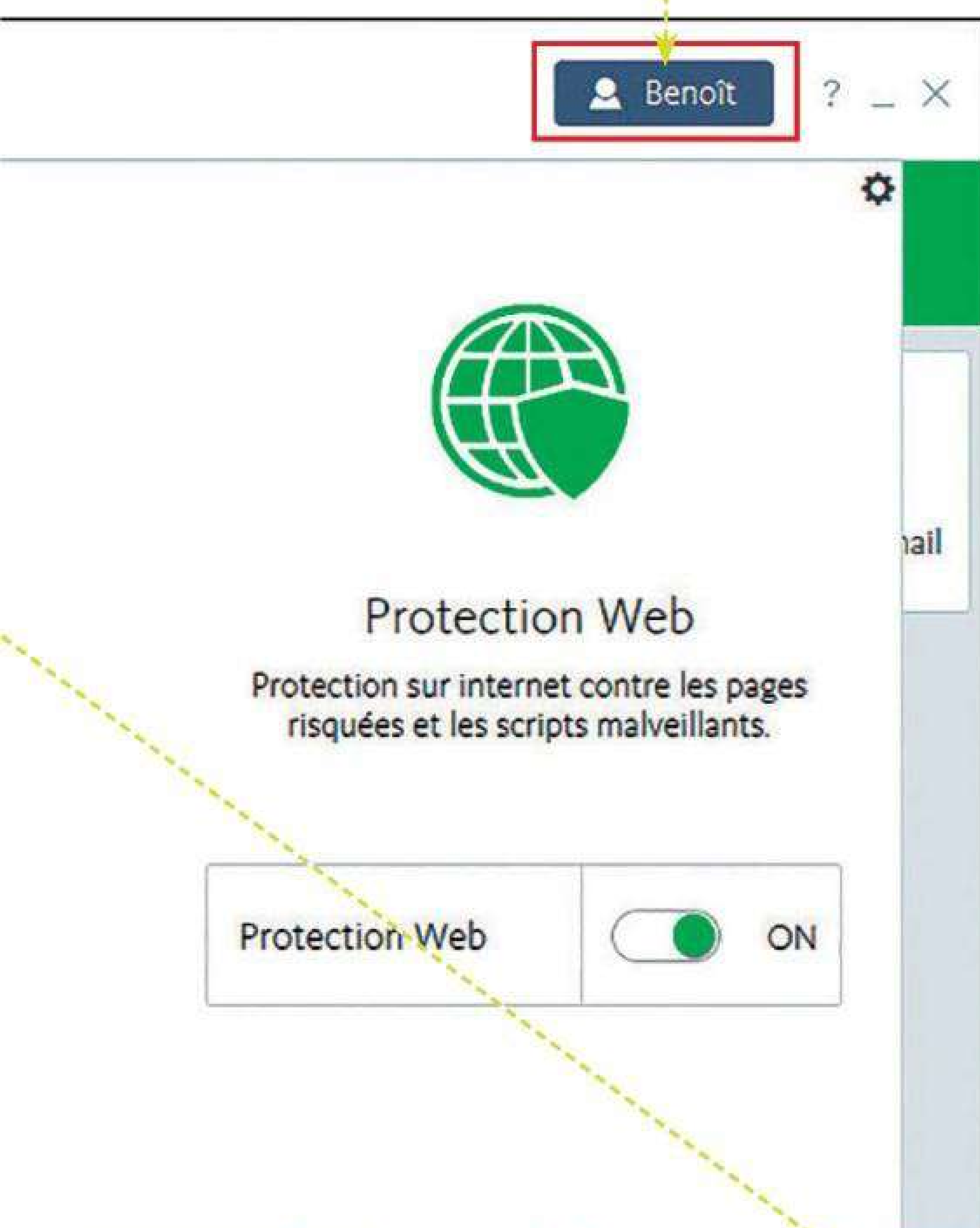


Ici vous retrouverez les éléments qu'Avira aura mis en quarantaine pour les isoler du système

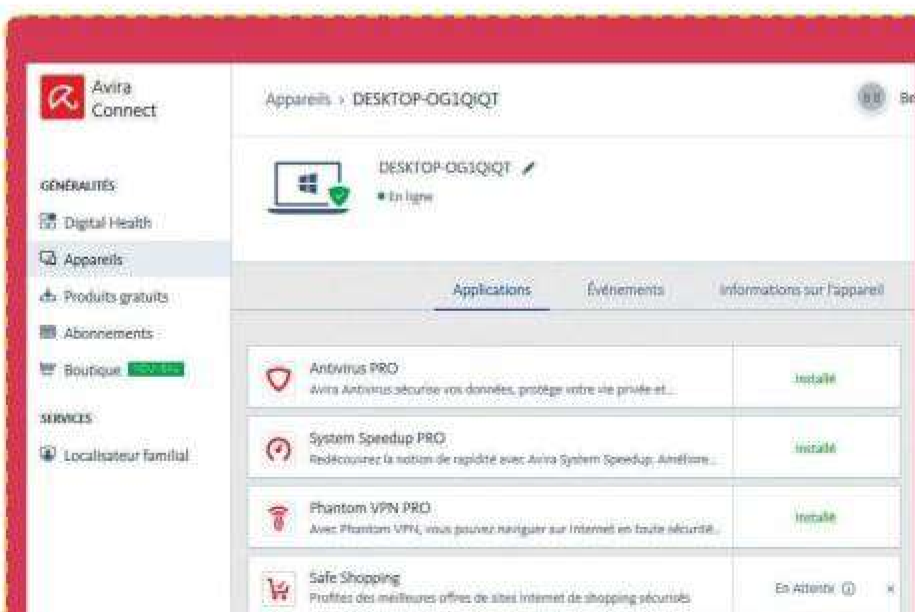
Vous trouverez ici les activités du programme : mise à jour, tâches, services activés, etc.



En ouvrant un compte, vous pourrez avoir accès à une interface Web permettant de gérer vos appareils, vos licences mais aussi de profiter de produits gratuits







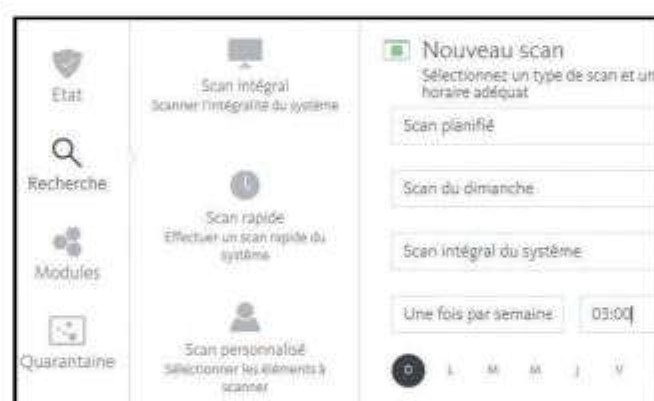
Les différents modules auxquels vous aurez accès dans la version payante (sauf la **Protection Temps Réel** qui est dispo dans la version gratuite. Notez qu'en ouvrant un compte, vous aurez le droit à une période d'essai pour la version Prime du logiciel mais aussi à des modules non présents à l'installation.

Avira gratuit et payant



01 › PREMIERS PAS

Dès le premierlancement, Avira va chercher les dernières signatures de virus et faire une mise à jour. Libre à vous de lancer votre premierscan avec Luke Filewalker, le système de recherche au nom désopilant.Sur la version gratuite, les options auxquelles vous n'avez pas accès sont notifiées en orange. Au lieu de proposer une fenêtre de paramétrage confuse, Avira a bien joué le coup.



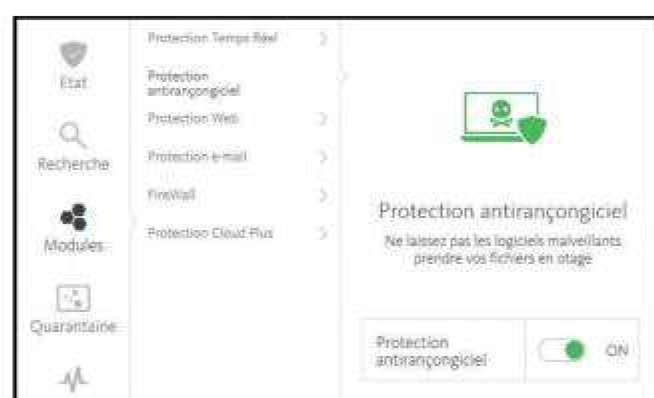
02 › LES TYPES D'ANALYSE

Dans l'onglet **Recherche**, vous pouvez choisir de faire un **Scan intégral**, un **Scan rapide**, un **Scan personnalisé** ou de planifier votre analyse. Notez que la protection en temps réel est de mise même pour la version gratuite. Si un malware est détecté, il peut être envoyé en quarantaine. Un doute sur une mise à jour ou une activité louche, vous trouverez un onglet dédié à gauche.



03 › LES OPTIONS PAYANTES

Dans les fonctions payantes, on compte le pare-feu très solide (il filtre par défaut les connexions entrantes, mais aussi sortantes) et facile à utiliser. Il suffit de cliquer sur **Autoriser** lorsqu'une application que vous connaissez va tenter de se connecter à Internet. Pour la protection e-mail, vous n'avez rien à faire, Avira va directement mettre un filtre sur les clients POP et IMAP (Windows Mail, Outlook, etc.)



04 › ANTI-RANSOMWARE

Avira Antivirus 2019 sait détecter des ransomwares nouveaux ou inconnus jusqu'ici et bloquer la progression des attaques avant qu'elles s'activent. Bien entendu, cela va de pair avec la gamme complète de techniques de détection d'Avira et l'apprentissage automatique avancé pour identifier et arrêter un large éventail de menaces entrantes.



05 › POUR LES UTILISATEURS AVANCÉS... ET LES AUTRES

Les paramètres de configuration sont très nombreux. Il est, par exemple, possible de régler la priorité de la fonction scanner, les actions à accomplir en cas d'infection, la spécification d'un mot de passe pour éviter que vos enfants ou des pirates ne désactivent vos protections, etc. Malgré tout, les débutants n'auront pas à s'arracher les cheveux puisque tout a été paramétré pour Monsieur Tout-le-Monde...

→ 4 SOLUTIONS ALTERNATIVES...

Même si vous avez un antivirus performant, vous pouvez aussi faire appel à des antimalwares spécialisés dans certains types d'attaque...

MALWAREBYTES



Face à certains virus particulièrement retors, votre antivirus généraliste risque d'être mis en échec. En cas d'infection, et régulièrement à titre préventif, Malwarebytes est une très bonne solution. Le logiciel dispose d'une période d'essai mais la version gratuite est très bonne. Si vous avez un doute sur la bonne tenue d'une désinfection, c'est le programme à utiliser.

Lien : **https://fr.malwarebytes.com**

ROGUEKILLER



Autre grand spécialiste de la chasse aux malwares, RogueKiller complétera utilement votre antivirus. À l'issue de l'examen (assez long), RogueKiller affiche la liste des logiciels indésirables et des anomalies qu'il a détectés, avec un code couleur indiquant leur niveau de dangerosité : rouge, orange, ou gris. Cochez celle en rouge ou orange et cliquez sur **Supprimer sélection**.

Lien : **https://goo.gl/Qr2YZ7**

ADWCLEANER

Les adwares encombrent votre navigateur, détournent vos recherches sur Internet, et affichent des encarts publicitaires dans Windows. Relativement



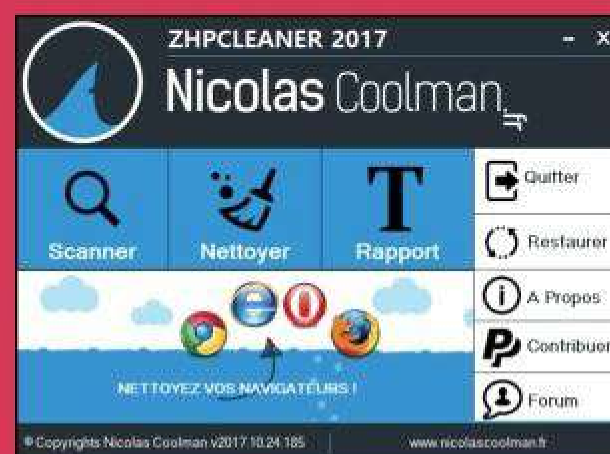
inoffensifs, ils sont souvent ignorés par les antivirus. AdwCleaner les élimine. Faire le ménage. L'analyse effectuée, cliquez sur **Nettoyer** pour éliminer les adwares détectés. Pensez à enregistrer vos éventuels travaux en cours avant de valider par **OK**.

Lien : **https://goo.gl/wkTy6a**

ZHP CLEANER

Vous rencontrez de plus en plus de problèmes avec votre navigateur : affichage de publicité, pop-up, barre de navigation non désirée ? Il s'agit peut-être de redirections d'URL (votre flux Internet passe par un proxy alors que vous n'avez rien demandé) et cela peut ouvrir la porte au phishing, à différents spywares ou pire...un botnet. ZHPCleaner va rétablir les paramètres proxy et supprimer les redirections d'URL sur tous vos navigateurs.

Lien : **www.nicolascoolman.com**



WINJA : LE PARTENAIRE DE VOTRE ANTIVIRUS !

Nous vous avions déjà parlé de Winja lorsque le logiciel est sorti il y a plusieurs mois déjà. Nous revenons dessus pour ce numéro car la société française Phrozen vient de lui ajouter certaines fonctionnalités. Rappelons que ce dernier permet d'éviter les contaminations et de surveiller un système potentiellement infecté. Un outil très complet permettant de scanner fichiers, URLs, services, programmes et tâches planifiées...



Phrozen SAS est une société française qui édite de nombreux logiciels de sécurité informatique : Who Stalks My Webcam pour surveiller l'activité de sa webcam, Windows Privacy Tweaker pour supprimer les mouchards de Windows 10, ADS Revealer qui se concentre sur une faille spécifique du système NTFS, RunPE Detector pour l'analyse de certains processus frauduleux et Shortcut Scanner pour surveiller les raccourcis Windows. Mais dans cet article, nous allons nous intéresser à Winja qui constitue le complément idéal à votre antivirus.

UN NINJA DANS VOTRE WINDOWS

Basé sur l'API Google Virus Total et développé de concert avec la firme américaine, Winja propose de soumettre n'importe quel fichier louche à une cinquantaine d'antivirus en ligne différents. Un doute sur un fichier avant de le télécharger ? Le logiciel va vérifier sa dangerosité avant même qu'il ne soit rapatrié sur votre ordinateur. Si « processus inconnu » vient apparaître dans votre gestionnaire des tâches, Winja ira se renseigner dans son immense base de données pour vous rassurer. Enfin d'autres outils vous permettront



«UNE FOIS QUE NOUS ACCEPTONS NOS LIMITES, NOUS LES DÉPASSONS» – ALBERT EINSTEIN



de mieux surveiller les planifications de tâches, les logiciels qui démarrent avec le système ou les services Windows qui peuvent aussi renfermer des saletés. Notez tout de même que Winja ne remplace pas un antivirus avec une protection d'arrière-plan. Par contre avoir les deux en même temps sur votre système ne causera aucun conflit... Bien sûr, tous les logiciels de chez Phrozen sont gratuits et sans publicité.



Dans la prochaine version de Winja, la société Phrozen va ajouter les fonctionnalités de Who Stalks My Webcam. Les deux logiciels ne feront alors plus qu'un !





INFOS [WINJA 5.1]
Où le trouver ? [**www.phrozen.io/freeware/winja**] Difficulté :

TUTO



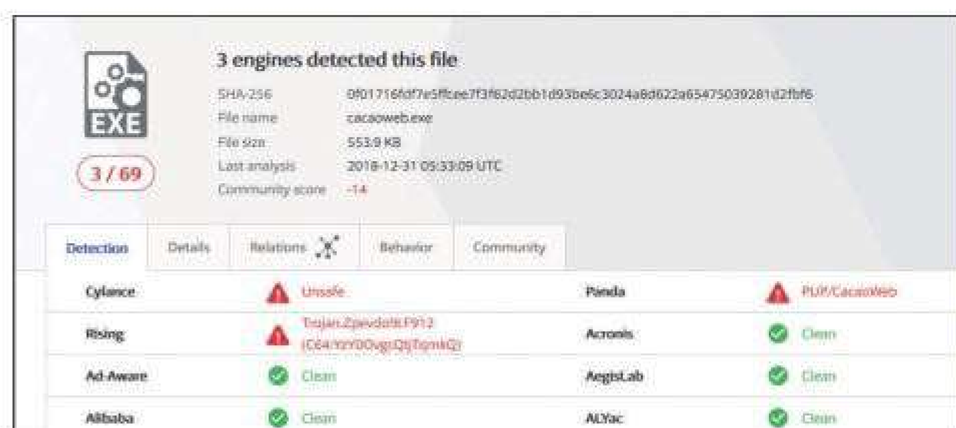
01 › L'INTERFACE

Après l'installation, l'interface va s'afficher avec ses différents boutons. Notez qu'il existe une version portable 32 ou 64 bits dans le ZIP où se trouve le fichier EXE. En vert vous trouverez l'option pour ouvrir un fichier déjà présent sur votre PC, en jaune pour scanner un fichier en ligne, en bleu pour les processus actifs et en rouge pour les outils complémentaires. Ces derniers doivent être lancés en mode administrateur (en faisant un clic droit sur l'icône de Winja).



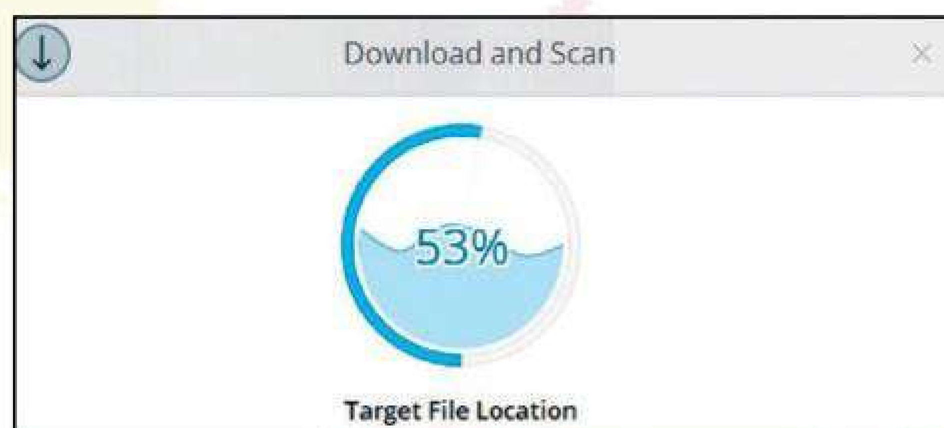
02 › NOTRE TEST

Pour tester, nous avons lancé un scan du controversé cacaoweb.exe. Le verdict est sans appel : infecté. Dès la fin du scan, une fenêtre vous proposera d'aller directement sur le site Virus Total. Vous pouvez aussi demander un nouveau scan ou voir les propriétés du fichier.



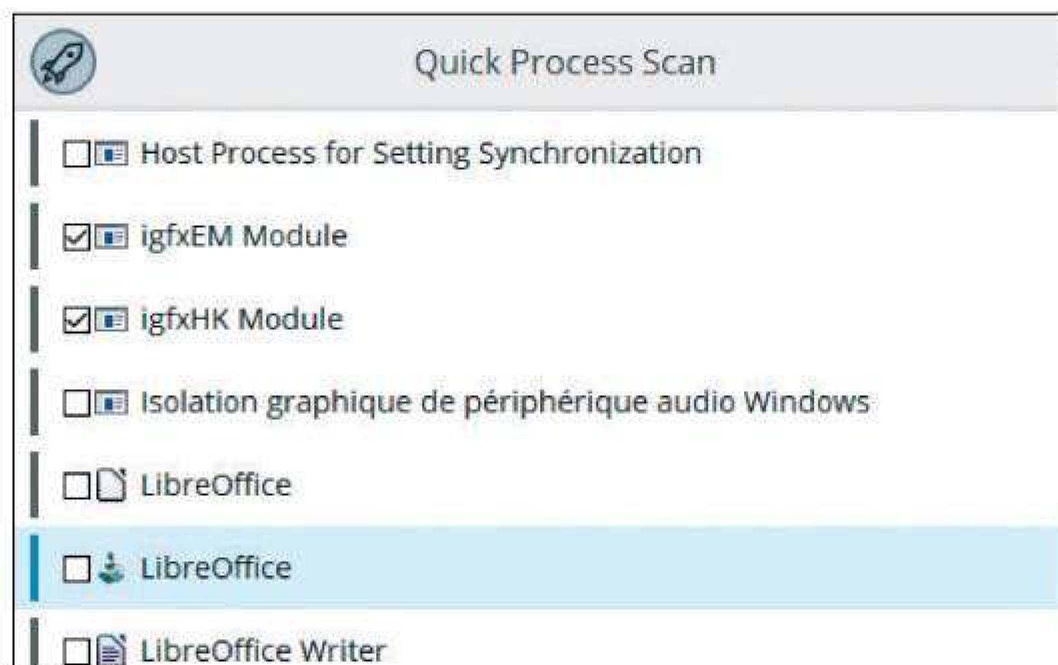
03 › 69 ANTIVIRUS À LA CARTE

En fait, 3 des antivirus de l'API Virus Total sur les 69 trouvent que ce programme de stream contient un PUP (Potentially Unwanted Program) ou un trojan: pas un virus ou un ver donc, mais une crotte de nez au mieux ou une belle saleté au pire. Même si la grosse majorité ne trouve rien à dire, il faudra se méfier. D'ailleurs Winja vous conseillera de lancer un scan avec votre antivirus. Notons qu'il peut aussi s'agir d'un programme «à décocher» lors de l'installation de cacaoweb. À vous de voir !



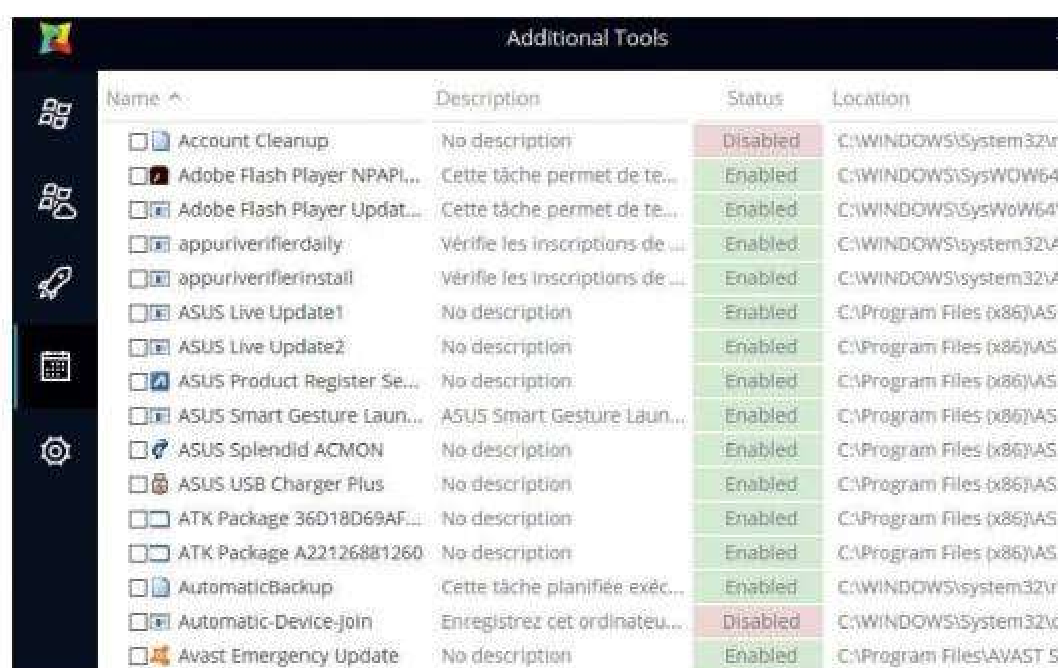
04 › SCANNER AVANT DE TÉLÉCHARGER

Vous êtes sur un site et on vous propose de télécharger un fichier EXE? Pourquoi prendre un risque? Depuis votre navigateur, faites un clic droit dans le bouton de téléchargement et faites **Copier l'adresse du lien** (ou équivalent). Dans Winja, allez dans **Download & Scan** puis copiez ce lien. Attendez le verdict.



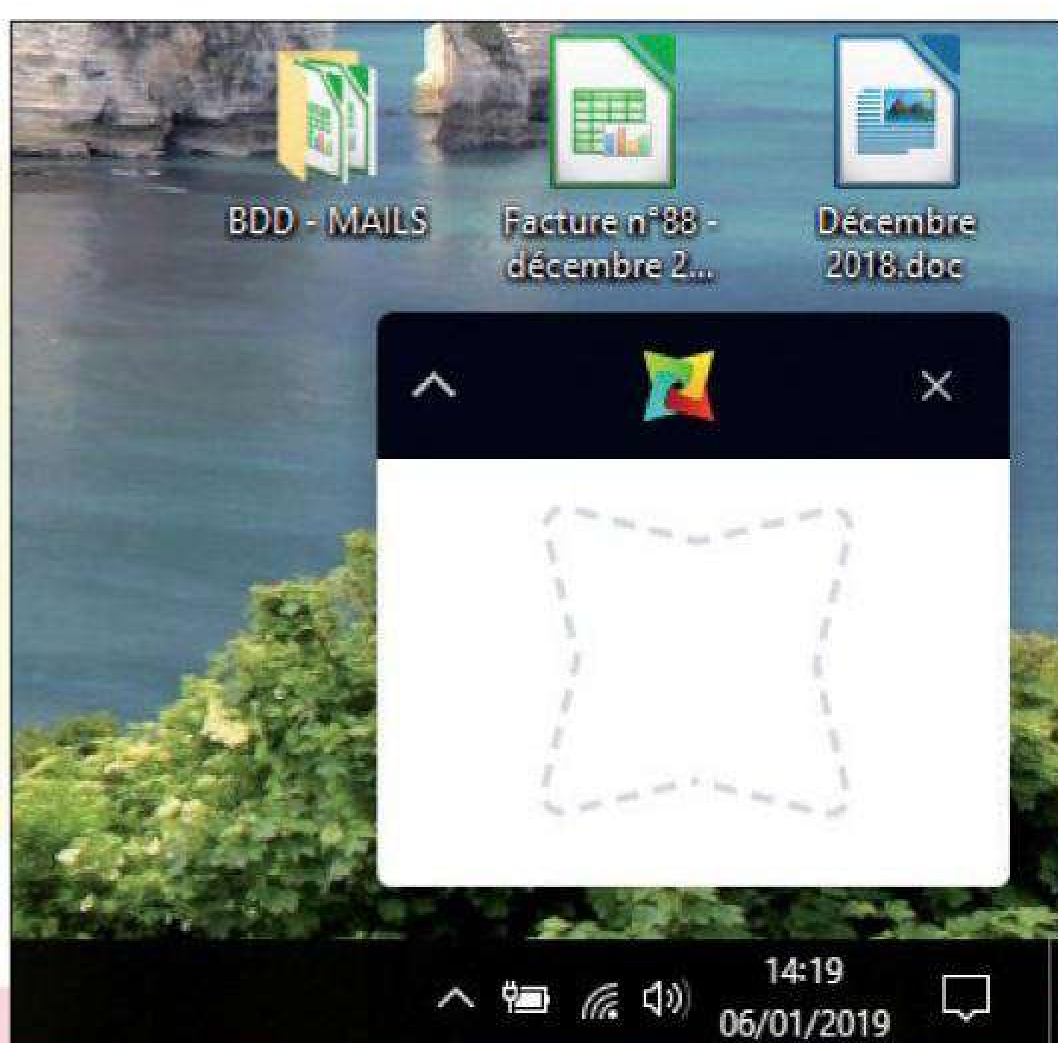
05 › RAPIDE !

Dans **Quick Process Scan**, sélectionnez les programmes qui tournent en arrière-plan sans pourtant se manifester. Vous pourriez avoir des surprises: des noms méconnus sont parfois parfaitement légitimes tandis que d'autres aux noms "passe-partout" sont des malwares. Notez que Winja est très rapide, car il se base sur les précédentes recherches des internautes en se fiant à l'empreinte unique de votre fichier (hash MD5 et SHA-1).



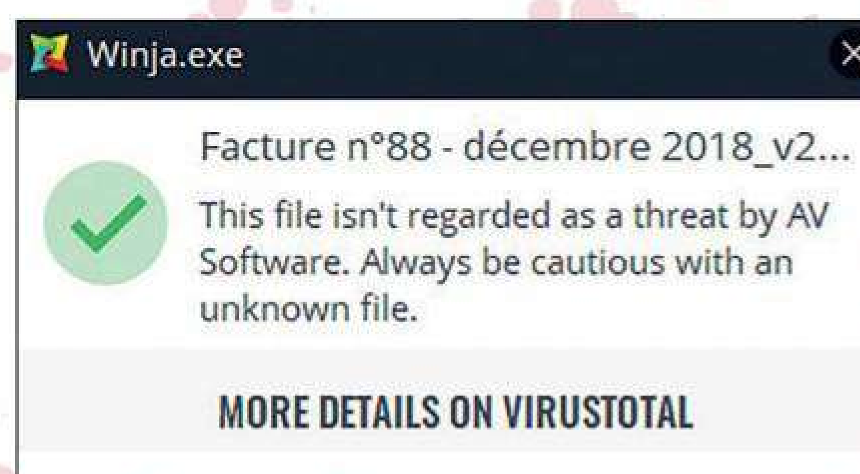
06 › DES OUTILS EN SUS

Enfin les **Outils supplémentaires** proposent un scan plus précis des processus, des tâches planifiées de Windows (qui peuvent être utilisées par des virus), des programmes qui se lancent au démarrage de Windows, et des services de Windows. Pour y accéder, il faudra juste accepter la proposition consistant à le lancer en mode administrateur.



07 › UN WIDGET SUR LE BUREAU

En réduisant le logiciel, un petit widget va s'afficher sur le bureau. Il s'agit d'une zone où vous pouvez glisser-déposer vos fichiers pour les analyser.



ESSAYER UN ANTIVIRUS EN LIGNE

En plus de l'antivirus installé sur votre PC, soumettez votre ordinateur à une analyse complémentaire, avec un antivirus en ligne comme F-Secure.





INFOS [F-SECURE]
Où le trouver ? [**www.f-secure.com**] Difficulté :

TUTO

F-Secure Online Scanner
Basé sur la technologie F-Secure Lighthouse
Cet outil recherche et élimine les applications et fichiers dangereux de votre ordinateur.
En cliquant sur le bouton Accepter et analyser, vous acceptez les Conditions d'utilisation.
Accepter et analyser

Analyse et nettoyage
Analyse c:\windows\system32\dmview.ocx
Analyse du système
41%
Analyse de la mémoire terminée

01 › ANALYSER

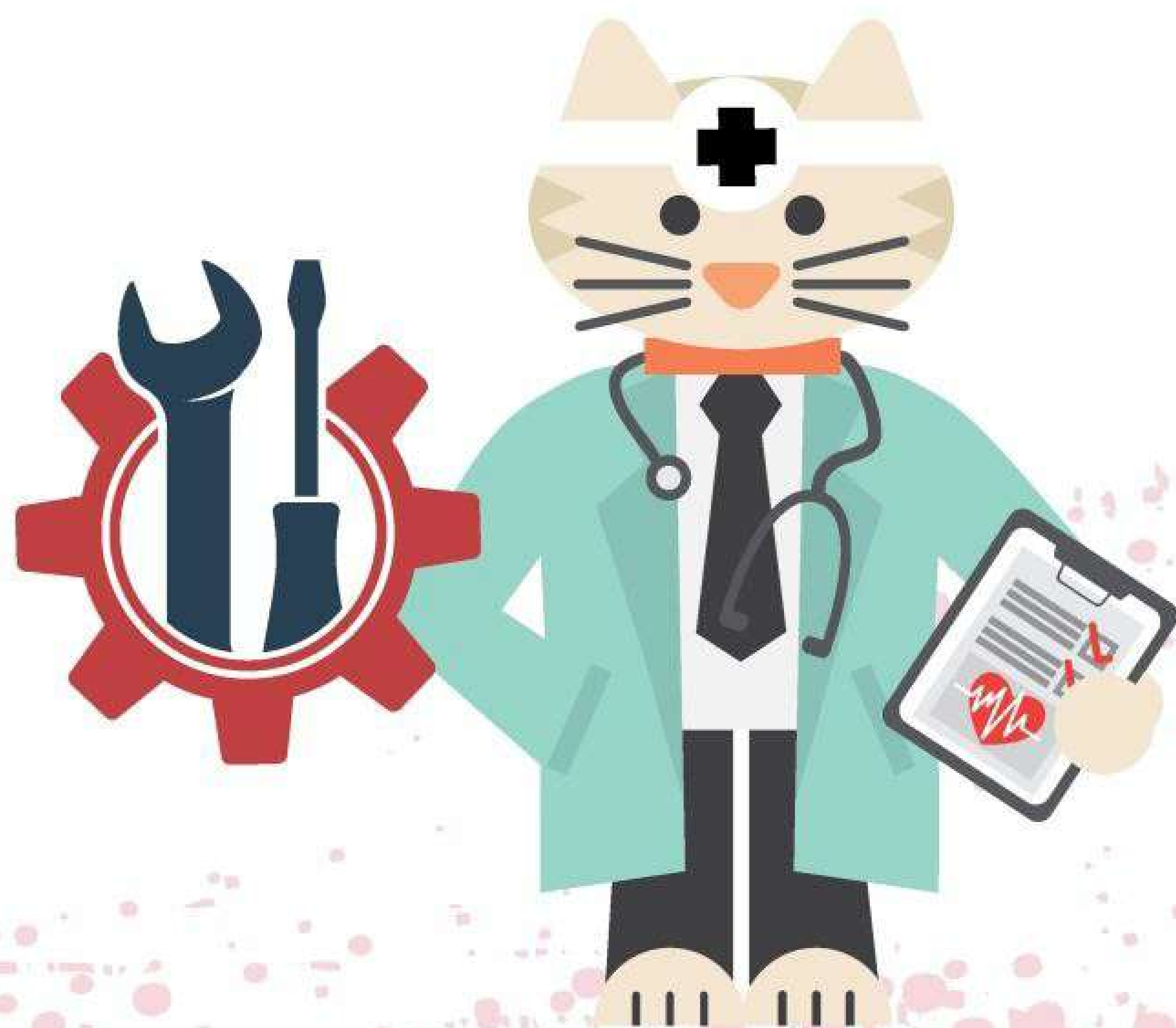
Sur la page d'accueil du service, cliquez sur Online Scanner – **Analysez et nettoyez gratuitement votre PC** puis **Lancer dès maintenant**. Acceptez le téléchargement du fichier proposé. C'est un exécutable, il n'y a rien à installer. Lancez-le et cliquez sur **Accepter et analyser**.

02 › NETTOYER

F-Secure analyse la mémoire de l'ordinateur puis le système entier. Patientez jusqu'à la fin de l'opération. Si le service détecte un fichier malveillant, il vous en informera et tentera automatiquement de le supprimer.

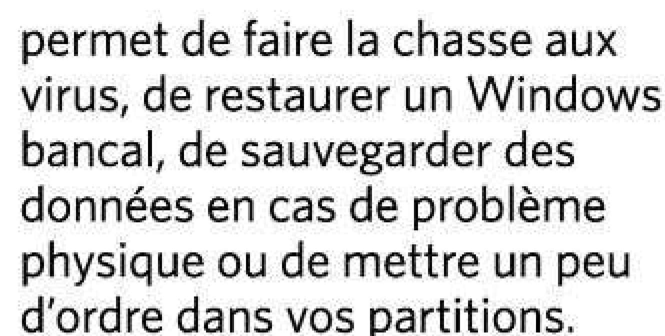
MEDICAT : LA TROUSSE À OUTILS UNIVERSELLE

Problème de fichier Windows, d'infection, de RAM, de disque dur, de partition ou de mot de passe ? Plus besoin d'avoir toute une collection de Live DVD sur vous lorsque vous partez réparer l'ordi de tata Lydie ou celui de Kévin (votre cousin de 13 ans qui se prend pour un hacker). MediCat propose une compilation d'outils fréquemment mise à jour...



Nous avons souvent parlé de Hiren's Boot CD, mais malheureusement, ce Live CD proposant une trousse à outils extrêmement complète n'est plus mis à jour et commence à se faire vieux. Pour remplacer cette compilation, nous vous proposons de découvrir MediCat (MediKit, MediCat, vous saisissez ?). Cette compilation




permet de faire la chasse aux virus, de restaurer un Windows bancal, de sauvegarder des données en cas de problème physique ou de mettre un peu d'ordre dans vos partitions.

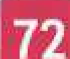
DES VERSIONS ENTRE 1,5 ET 7,5 GO

MediCat comprend aussi des outils de diagnostic en tout genre, plusieurs logiciels pour récupérer vos mots de passe (dont ceux de Windows et de certaines distributions Linux). Idéal pour les altruistes qui n'hésitent pas à se déplacer pour réparer l'ordi d'un ami, MediCat est indispensable. La version la plus «lourde» peut aisément prendre place sur une vieille clé USB de 8Go, raison de plus pour la garder tout le temps avec soi.

L'auteur du logiciel refuse les dons, mais il ne roule pas sur l'or. Il ne dispose même pas d'un site pour y déposer son œuvre. À la place, il utilise Google Drive ou Mega. Pas besoin de s'inscrire, mais le téléchargement est un peu laborieux. C'est là le moindre défaut de MediCat...

BIOS UEFI ?

Certains fabricants de cartes mères intègrent depuis quelques années un BIOS sécurisé et un peu pénible appelé UEFI ou EFI. Ce BIOS spécial est un peu difficile à prendre en main et vous donnera du fil à retordre si vous souhaitez «booter» depuis un CD, un DVD. Dans ce cas, il faudra désactiver l'option Secure Boot et activer le Boot Legacy (ou CSM si cette dernière est présente). Pour les clés USB, le logiciel Rufus (voir notre pas-à-pas) vous facilite un peu la tâche même si cela ne fonctionne pas encore à 100%. Pour en savoir plus et apprendre comment s'en sortir avec ces BIOS, voici un article très intéressant : **http://goo.gl/KSDTS5**





INFOS **[MEDICAT]**
Où le trouver ? [**https://goo.gl/3imeh8**]



[RUFUS] Où le trouver ? [**https://rufus.akeo.ie**] Difficulté :

TUTO





01 › L'IMAGE ISO

Choisissez la version que vous voulez sur le Google Drive ou Mega. Nous vous conseillons la plus lourde sauf si vous n'avez pas de graveur de DVD double densité (et pas de clé USB). Notez qu'il faudra rassembler les fichiers (**medicat.16.10.stable.7z.001**, **medicat.16.10.stable.7z.002**, etc.) avec 7-Zip en ouvrant le premier. Gravez celte image ou ouvrez Rufus, laissez **MBR pour BIOS ou UEFI**, **FAT32** comme système de fichier et choisissez **Image ISO** dans le dernier menu déroulant. Dans la case à droite, renseignez l'emplacement de l'image. Faites **Démarrer** mais attention, votre antivirus va sans doute se réveiller. Désactivez-le pendant cette phase.

02 › «BOOTER» DEPUIS UN PÉRIPHÉRIQUE

Pour booter sur le lecteur DVD ou sur un port USB, il faudra juste demander à votre PC de le faire. Faites **Suppr**, **F1**, **F2** ou **F8** (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** (qui peut aussi être sélectionnable avant même l'entrée dans les menus) et modifiez l'ordre en mettant en premier votre lecteur optique ou l'USB. Pour les BIOS UEFI, consultez notre encadré à ce sujet...



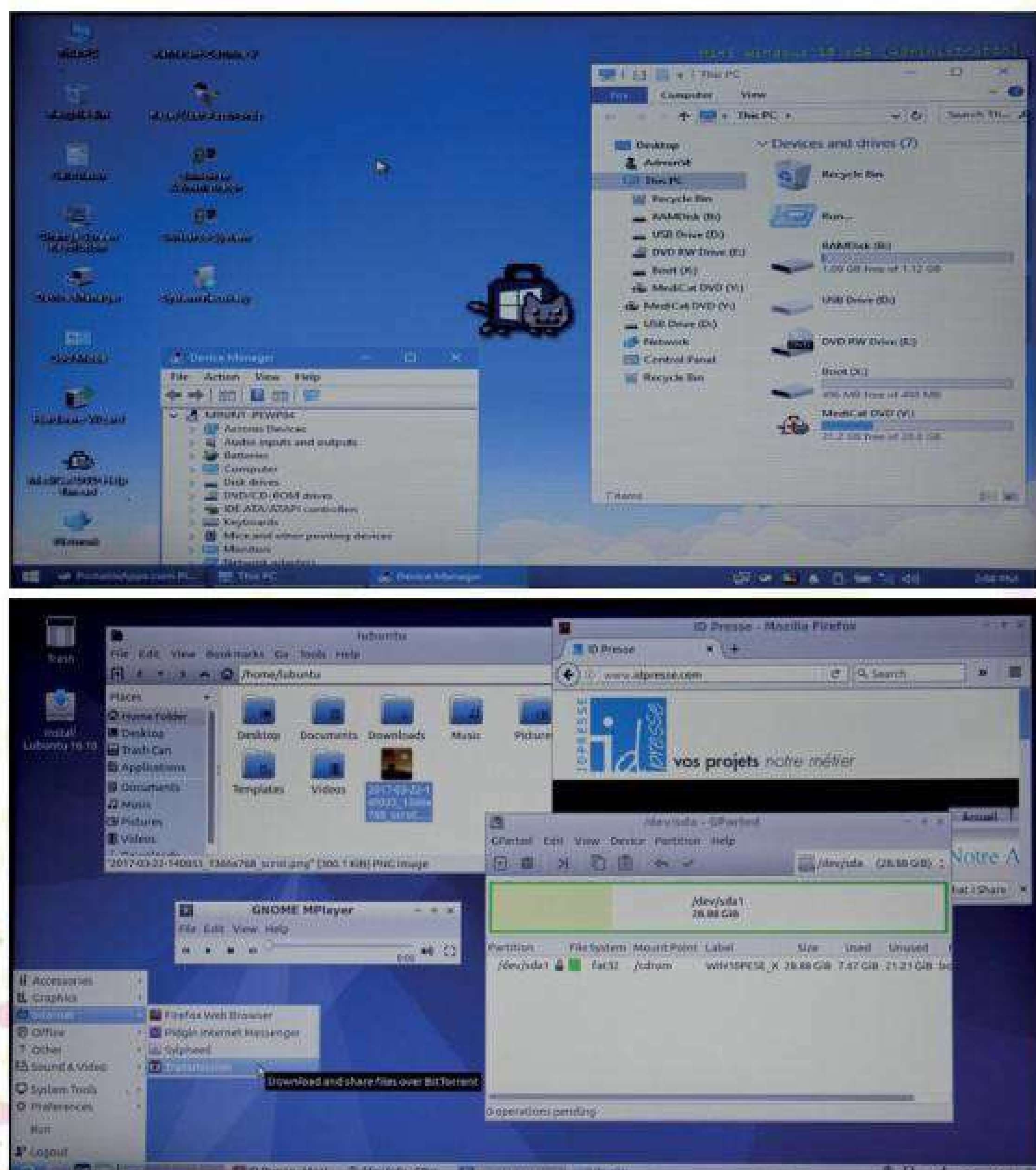
03 › LE MENU PRINCIPAL

Vous devriez voir l'interface principale avec **Continue Booting The PC** (pour booter normalement sur le disque dur une fois que vous aurez terminé), **Boot Other Harddisk Partitions** pour choisir sur quelle partition booter (au cas où vous auriez plusieurs OS sur lesquels démarrer) et **64-Bits Windows Recovery** pour retrouver un Windows stable. Ensuite nous avons **Diagnostic Utilities** avec **Hardware Detection Tool** (pour identifier les périphériques et mieux choisir ses pilotes), **MemTest**, **TestDisk** (voir page xx) et le classique **Ultimate Boot CD**.



04 > ANTIVIRUS ET ACCÈS WINDOWS

En cas d'infection, c'est **Scan for Viruses** qu'il faudra sélectionner. Cette option va afficher l'antivirus Comodo. Depuis cette interface vous pourrez bien sûr lancer des scans, mais aussi accéder à Internet et à des outils rudimentaires (navigateur, capture d'écran, etc.) **Remove User Account Password** vous donne accès à des outils que nous avons déjà abordés, dont **Offline NT Password & Registry Editor** (*Les Dossiers du Pirate* n°10) et **Kon-Boot** (*Pirate Informatique* n°28) qui permettent de retrouver un accès à Windows si vous avez oublié votre mot de passe de session. Ces logiciels ne fonctionnent qu'avec le mot de passe local et pas du tout avec le nouveau type de mot de passe Compte Microsoft.

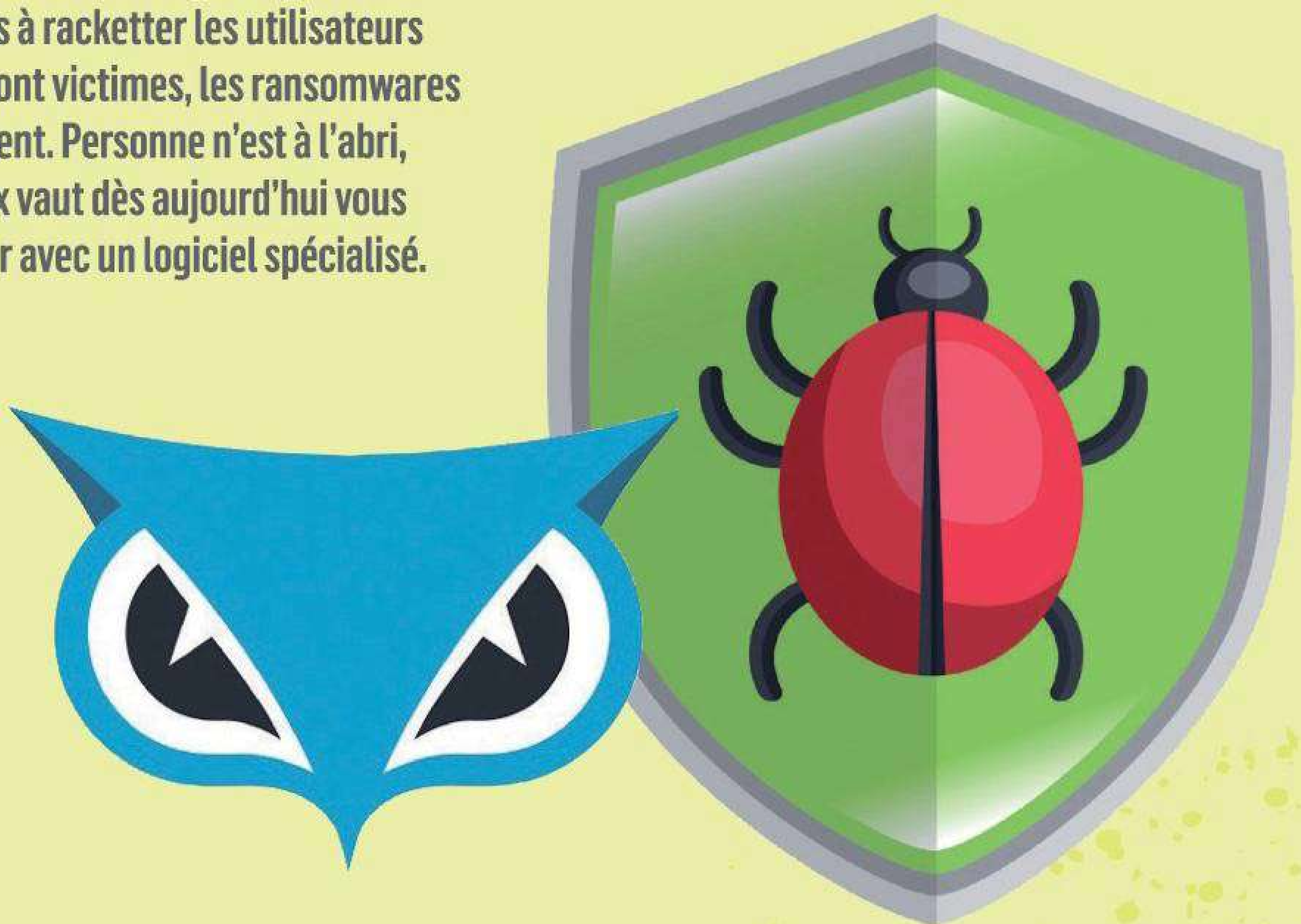


05 > DEUX OS EN PRIME

Là où Hiren's Boot CD donnait l'accès à un Windows XP «light», MediCat propose un **Mini Windows 10** et **Lubuntu**. Le premier vous donne un véritable petit Windows pour récupérer ce qui peut l'être, accéder au réseau, gérer vos périphériques, monter des disques durs et tout ce qu'on peut faire avec un véritable OS graphique. Il comprend aussi la collection de logiciels de **PortablesApps.com** pour réparer, sauvegarder, etc. Lubuntu fera la même chose pour les linuxiens puisqu'il s'agit d'un Ubuntu «light» avec à peu près les mêmes options, mais pour les systèmes au manchot. **MediCat FreeDOS** n'a quant à lui que très peu d'intérêt puisqu'il s'agira d'aller dépanner les anciens systèmes ou de fonctionner sur de très modestes configurations.

PROTÉGEZ-VOUS DES RANSOMWARES

Destinés à racketter les utilisateurs qui en sont victimes, les ransomwares prolifèrent. Personne n'est à l'abri, et mieux vaut dès aujourd'hui vous protéger avec un logiciel spécialisé.



Les ransomwares ou rançongiciels sont des malwares introduits par un ver informatique. Une fois installés sur votre PC, ils ciblent les types de fichiers correspondant à vos données personnelles (photos, vidéos, documents DOC ou XLS, etc.), et les chiffrent avec une double clé très solide. Au bout de quelques minutes, vos documents deviennent inaccessibles et un message s'affiche sur votre écran, vous invitant à payer une somme d'argent pour récupérer la clé privée qui a servi au chiffrement et ainsi retrouver vos données. S'il est parfois possible d'agir après le chiffrage des données via des programmes spécifiques (voyez l'étape page suivante), il est important de se protéger. Antivirus spécialisé, le logiciel RansomFree se base sur l'analyse de 40 ransomwares et leurs variantes connues. Dès que le schéma typique d'un tel programme est détecté, RansomFree bloque le processus de chiffrement. Notez qu'il ne vous empêche pas d'utiliser des logiciels de chiffrement comme VeraCypt ou AxCrypt.



INFOS [RANSOMFREE]
Où le trouver ? [**https://ransomfree.cybereason.com**] Difficulté : ☠☠☠

TUTO





01 › INSTALLER RANSOMFREE

Une fois installé, RansomFree va disséminer des fichiers leurres (des sortes d'appâts inoffensifs en somme) aux quatre coins de votre disque dur. Si un ransomware tente de chiffrer vos données, il ira aussi s'attaquer à ces fichiers et déclenchera l'alerte. Vous n'avez rien à faire ni aucun réglage à effectuer.

02 › LAISSER FAIRE LE LOGICIEL

RansomFree n'est pas actif, puisqu'il agit en silence et qu'il n'apparaît pas dans la liste des programmes en cours du Gestionnaire des tâches. Rassurez-vous : RansomFree démarre systématiquement en même temps que Windows. Notez qu'il fonctionne aussi si un disque dur réseau est attaqué.





03 › RÉAGIR AUX ALERTES

En cas d'alerte, le processus incriminé est suspendu, stoppant net le chiffrement frauduleux de vos données. Vous pouvez voir la liste des fichiers attaqués (**View affected files**), choisir de laisser faire (**No, Let it run**) s'il s'agit d'une fausse alerte, ou au contraire bloquer définitivement le processus et faire le ménage (**Yes, Stop & clean the threat**).

04 › AGIR EN CAS D'INFECTION

Le site www.nomoreransom.org centralise tout ce qu'il faut savoir sur ces malwares au niveau de la prévention, mais il dispose aussi d'un service de détection en ligne (pour savoir de quel mal vous avez hérité) et de plusieurs outils de déchiffrement. Ce sont plus de 25 ransomwares qui peuvent être éradiqués avec ces outils.

RÉCUPÉREZ vos DONNÉES

Victime d'un ransomware, vous vous retrouvez avec des fichiers chiffrés auxquels vous ne pouvez plus accéder ? Essayez Ransomware File Decryptor.







INFOS [RANSOMWARE FILE DECRYPTOR]
Où le trouver ? [**https://goo.gl/b7UxEw**] Difficulté : ☠☠☠

TUTO



Anti-Ransomware
Trend Micro experts help you decrypt your encrypted files

1 Select the ransomware name

Select

Ransomware Name
Select the ransomware name

○ TeslaCrypt (V3,V4)	○ BadBlock
○ CryptXXX	○ 777
○ SNSLocker	○ XORIST
○ AutoLocky	○ XORBAT
○ CERBER(V1)	○ STAMPADO

01 › DÉSIGNER LE COUPABLE

Ne nécessitant pas d'installation, Ransomware File Decryptor est un logiciel très facile à prendre en main. Acceptez le contrat d'utilisation (**Agree**) puis sélectionnez le ransomware dont vous êtes la victime. Si vous ne connaissez pas le nom, cherchez sur Internet l'extension de fichier qui apparaît ou voyez le site **www.nomoreransom.org**.

02 › DÉCRYPTER UN FICHIER

Notez qu'on trouve même WannaCry dans la liste ! Faites ensuite **Select & Decrypt** pour sélectionner un fichier chiffré avec ce ransomware. Au bout de quelques secondes, Ransomware File Decryptor va vous rendre votrefichier d'origine.



01# Vacciner ses périphériques USB
→ AVEC USB FIX

Les virus dits « autorun » infectent les périphériques USB. Dès que vous les connectez à votre machine, ils entrent en action. USB Fix permet de s'en protéger. Ouvrez le programme et cliquez sur **Vacciner** puis suivez les instructions à l'écran. Désormais, les périphériques USB concernés ne peuvent plus lancer les programmes « autorun » (qu'ils soient néfastes ou non).

Difficulté : Lien : **www.usb-antivirus.com**



02# Exploiter un antivirus en ligne
→ AVEC SECUSER

Besoin d'un scan rapide sur une machine qui ne possède pas d'antivirus ? Ou d'une analyse complémentaire à celle de votre antivirus ? Passez par un service en ligne comme Secuser. Après avoir choisi la bonne version (32 ou 64 bits), lancez le fichier **.exe** téléchargé et patientez le temps de l'analyse.

Difficulté :

Lien : **www.secuser.com/antivirus**



03# Contrer les ransomwares
→ AVEC ID RANSOMWARE



Les vils ransomwares cryptent vos documents pour vous soutirer de l'argent en échange de la clé les déverrouillant (et encore, ce n'est pas garanti !). Via ce site, vous identifiez votre ransomware en téléversant un des fichiers cryptés à l'aide de **Parcourir** (sous **Échantillon de fichier chiffré**). Une fois les informations envoyées, le site vous souffle la solution pour récupérer vos données. Si elle existe...

Difficulté :

Lien : **https://goo.gl/AhQXKo**

04# Scanner les ports du PC

→ AVEC INOCULER

Vous pensiez être totalement protégé, mais vous avez quand même réussi à attraper un virus sur votre PC ? La faille est probablement liée à un port laissé ouvert. Depuis le site, cliquez sur **Scanner les ports de mon ordinateur maintenant**. Les ports laissés ouverts sont notés en rouge, à vous de les fermer via votre pare-feu. Notez que le rôle de ce scanner étant de tester la sécurité de votre machine, votre pare-feu peut croire à une attaque. Fausse alerte, vous ne risquez rien.

Difficulté : ☠☠☠ Lien : **www.inoculer.com/scannerdeports.php**

05# Repérer les vulnérabilités

→ AVEC MICROSOFT BASELINE SECURITY ANALYSER

Microsoft Baseline Security Analyser (MBSA) récupère depuis les serveurs Microsoft les dernières informations publiées sur les failles et patchs de sécurité. Il teste tous les points du système susceptibles de présenter une faille de sécurité (comptes actifs, solidité des mots de passe, présence des patchs, logiciels récemment installés, configuration du pare-feu, etc.). Pour chaque point contrôlé, si la sécurité semble insuffisante, voire défaillante, le logiciel explique comment mettre en oeuvre la parade adéquate.

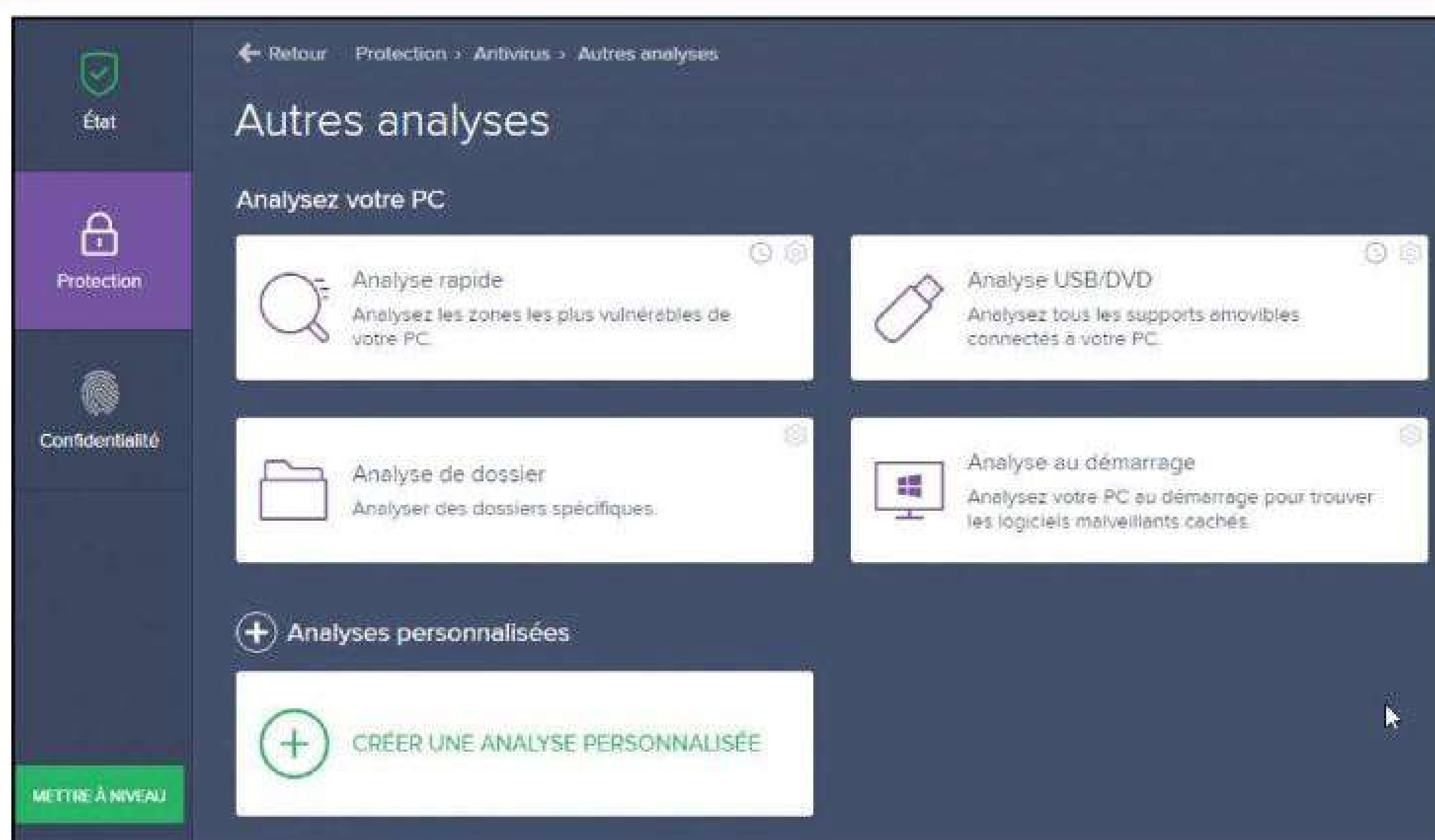
Difficulté : ☠☠☠ Lien : **http://goo.gl/UBHss**



06# Vérifier un périphérique USB

→ Avec Avast

Si vous branchez sur votre PC une clé ou un disque que quelqu'un vous a prêté (ou lorsque vous récupérez une clé ou un disque que vous avez vous-même prêté), ne manquez pas de vérifier que le périphérique n'embarque pas un invité indésirable. Avast possède justement un outil pour analyser les périphériques USB. Allez dans **Protection > Antivirus > Autres Analyses > Analyse USB/DVD**.



Difficulté : ☠☠☠ Lien : **www.avast.com**

07# Installer un antivirus léger et efficace

→ Avec Microsoft Security Essentials

Vous cherchez un antivirus léger, discret et simple, qui n'affecte pas les performances de votre PC et n'exige aucun réglage ? Les antivirus de Microsoft font parfaitement l'affaire, et sont assez efficaces, contrairement à ce que prétendent certains. Windows Defender est fourni avec Windows 10, vous n'avez besoin de rien de plus. Si vous êtes sous Windows 7, installez Microsoft Security Essentials.

Microsoft Office Windows Surface Xbox Offres spéciales Support technique Plus

Support Microsoft

Téléchargement de Microsoft Security Essentials

S'applique à : Windows 7

Protection pour votre PC

Windows Defender est intégré à la dernière version de Windows et vous aide à protéger votre PC contre les virus et autres programmes malveillants.

Si votre PC exécute une version plus ancienne de Windows 7, vous pouvez télécharger Microsoft Security Essentials et ce, gratuitement !

Éléments inclus

	Microsoft Security Essentials Windows 7	Windows Defender Windows 8,Windows RT, Windows 8.1, Windows RT 8.1, Windows 10
Protection en temps réel contre les logiciels espions, les virus, les rootkits et	x	x

Difficulté : ☠☠☠ Lien : **http://goo.gl/4vsTk**

SAUVEGARDE



p82
SAUVEGARDER votre système et vos données

p88
Toutes nos pistes pour vos **SAUVEGARDES**

p92
Une **IMAGE MIROIR** de votre disque dur avec TestDisk

p96
RÉCUPÉREZ photos et fichiers perdus !

p98
SAUVEGARDEZ dans le **CLOUD**

SAUVEGARDER VOTRE SYSTÈME ET VOS DONNÉES



Vous n'êtes pas à l'abri d'une défaillance grave du système et dans ces cas-là, c'est toute votre vie numérique qui peut se trouver menacée. Pour récupérer vos données en cas de pépin, ou redémarrer votre ordinateur s'il est bloqué, planifiez des sauvegardes régulières.

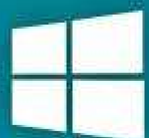
Si vos soucis d'ordinateur ont commencé avec l'installation d'un programme, c'est que ce dernier a sans doute quelque chose à voir avec le problème. Il faudra tenter une désinstallation « propre » depuis le module de Windows, et peut-être passer par un utilitaire spécialisé. Si au contraire un logiciel refuse de s'installer, méfiez-vous du distinguo 32/64 bits qui peut parfois semer la discorde dans le système. N'oubliez pas l'adage : « Qui peut le plus, peut le moins ». Un système 64 bits fera tourner du 32 ou du 64 bits sans problème tandis qu'un système 32 bits sera cantonné aux programmes conçus pour lui. Choisissez bien la version de votre programme ! Enfin si votre programme s'installe mais ne fonctionne pas parce qu'il est trop vieux (sorti à l'époque de Windows XP, voir avant), Windows a plus d'un tour dans son sac et vous proposera de remonter dans le temps.

AVEC WINDOWS 8 ET 10



Les captures qui illustrent notre article ont été réalisées avec la version 7 de Windows, mais Windows 8 et 10 permettent de faire exactement la même chose. Il suffit d'aller dans le **Panneau de configuration**, de trouver l'application **Historique des fichiers** et de l'activer (après avoir branché un périphérique de stockage externe). Comme pour Windows 7, l'opération va sauvegarder par défaut vos bibliothèques, vos contacts, vos favoris, etc. Il est bien sûr possible de choisir soi-même ces éléments, d'en exclure et de planifier les sauvegardes dans les **Paramètres avancés**.



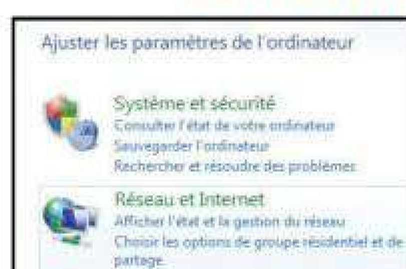


INFOS [MODULE DE SAUVEGARDE DE WINDOWS]
Où le trouver ? [**www.microsoft.com**] Difficulté :

TUTO

CONFIGURER LA SAUVEGARDE

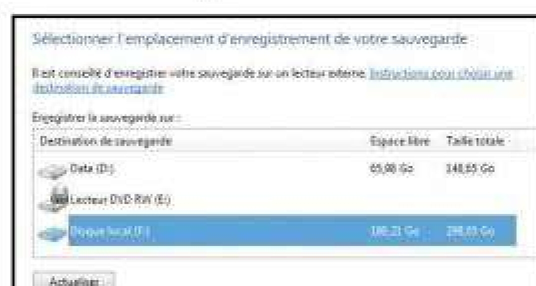
01 › OUVRIR LE PANNEAU DE CONFIGURATION



La première étape consiste à ouvrir le **Panneau de configuration** et à cliquer sur **Sauvegarder l'ordinateur** dans la partie **Système et sécurité**. Dans la nouvelle fenêtre, cliquez sur **Configurer la sauvegarde** (attention, il faut que vous soyez l'administrateur du PC). On vous demandera alors de choisir l'emplacement de votre sauvegarde.

02 › INDIQUER L'EMPLACEMENT

Le mieux est de réaliser la sauvegarde sur un disque dur externe ou une clé USB, qui sera tout le temps branché à votre PC pour que les prochaines sauvegardes puissent s'effectuer automatiquement en fonction de votre planning. Notez qu'il est possible de faire une sauvegarde à travers le réseau si vous êtes connecté à un réseau local.



03 › CHOISIR LES ÉLÉMENTS

On vous demandera alors ce que vous désirez sauvegarder. Vous pouvez laisser Windows décider pour vous (le système sauvegardera vos bibliothèques, vos favoris, les documents du bureau, etc.), mais nous vous conseillons de faire les choix à la main pour éviter les oublis : faites **Me laisser choisir** puis **Suivant**.



04 › VÉRIFIER LA SÉLECTION

Dans notre exemple, nous avons choisi de sauvegarder les **Bibliothèques** de Windows (**Images, Documents, Musique** et **Vidéos**) pour tous les utilisateurs du PC. Mais rien ne vous empêche de fureter dans vos disques durs à la recherche d'autres dossiers à sauvegarder, il suffit de cocher les cases.

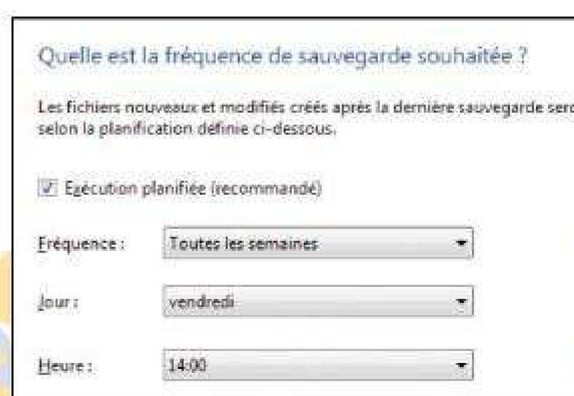
05 › SAUVEGARDER LE SYSTÈME

Notez que c'est à ce moment que vous pouvez choisir d'inclure une image système, en plus de vos documents et données personnelles. Cochez pour cela la case **Inclure une image système**... (notez que cette option n'est fonctionnelle que si votre support de sauvegarde est formaté en NTFS, et non en FAT).



06 › PLANIFIER ET LANCER

Faites **Suivant** pour accéder à **Modifier la planification**. Vous pouvez choisir la fréquence des sauvegardes, le jour de la semaine et même l'heure. Faites **Enregistrer les paramètres et exécuter la sauvegarde** pour lancer la première sauvegarde.
À titre d'exemple, une sauvegarde de 40 Go demande environ une heure.



RESTAURER UNE SAUVEGARDE





01 › OUVRIR LE PANNEAU DE CONFIGURATION

Après un problème de matériel ou une réinstallation, vous désirez restaurer des fichiers que vous avez placés en lieu sûr ? Ouvrez le **Panneau de configuration** et cliquez sur **Sauvegarder l'ordinateur** dans la partie **Système et sécurité**. Cette fois, dirigez-vous vers la seconde partie et cliquez sur **Restaurer mes fichiers**.

02 › CHOISIR LA SAUVEGARDE

Si vous avez plusieurs sauvegardes, faites **Rechercher** pour trouver la dernière en date. Dans **Dossier**, sélectionnez le dossier de sauvegarde et faites **Suivant**. Dans la fenêtre suivante, il est possible de sélectionner l'emplacement de restauration des fichiers. Vous pouvez choisir l'emplacement d'origine des données.





03 › LANCER LA RESTAURATION

Faites **Restaurer**. Si des fichiers déjà présents sur le disque portent le même nom qu'un fichier de la sauvegarde, Windows vous demandera si vous souhaitez écraser le plus vieux ou si vous voulez le dupliquer. À la fin du processus, vous aurez retrouvé vos précieux fichiers, à l'emplacement demandé.

04 › RESTAURER LE SYSTÈME

Pour restaurer le système à un état antérieur, il faut choisir **Restaurer les paramètres système**... à l'étape 1. Vous devez ensuite choisir une image système depuis Windows ou depuis votre périphérique. Le principe est le même que pour les points de restauration.

EN CAS DE BLOCAGE

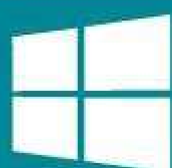


Si Windows ne veut même plus démarrer, impossible d'aller dans le **Panneau de configuration** pour récupérer une sauvegarde ! Dans ce cas, il faut lancer le système à partir du DVD d'installation de Windows, qui vous permettra ensuite de restaurer système et données. Si vous ne possédez pas ou plus ce DVD, créez dès à présent un disque de secours en faisant **Créer un disque de réparation système** depuis la fenêtre de configuration des sauvegardes.

ACTIVEZ L'HISTORIQUE DES FICHIERS



Depuis Windows 8, une nouvelle fonction vous permet de retrouver les versions antérieures de vos documents. Pratique en cas de suppression accidentelle.



INFOS [WINDOWS] Difficulté : ☠

TUTO

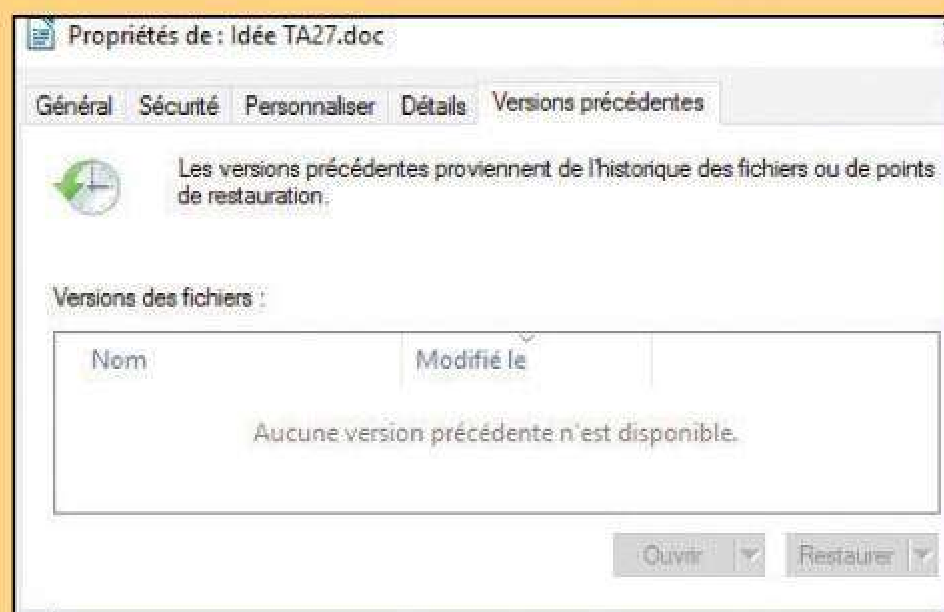
Sauvegarder à l'aide de l'historique des fichiers

Sauvegardez vos fichiers sur un autre lecteur, puis restaurez-les si les originaux sont perdus, endommagés ou supprimés.

Sauvegarder automatiquement mes fichiers

Activé

Plus d'options



01 › ACTIVER L'HISTORIQUE

Branchez un périphérique externe (disque dur ou clé USB) destiné à accueillir les sauvegardes, et allez dans **Paramètres du PC > Mise à jour et sécurité > Sauvegarde** puis **activez l'historique des fichiers**. Cliquez sur **Plus d'options** pour choisir la fréquence de sauvegarde, la durée de conservation de ces dernières et les dossiers à inclure/exclure du processus.

02 › RETROUVER LES ANCIENNES VERSIONS

Si le fichier existe encore, faites un clic droit dessus puis **Propriétés** et **Versions précédentes**. Choisissez-en une et validez avec **Restaurer**. Le fichier a été effacé ? Retournez dans **Paramètres du PC > Mise à jour et sécurité > Sauvegarde**, cliquez sur **Plus d'options** et, tout en bas, **Restaurer les fichiers à partir d'une sauvegarde en cours**.

LE MAILING-LIST OFFICIELLE de

Pirate Informatique et des *Dossiers du Pirate*

INSCRIVEZ-VOUS GRATUITEMENT !

De nombreux lecteurs nous demandent chaque jour s'il est possible de s'abonner. La réponse est non et ce n'est malheureusement pas de notre faute. En effet, nos magazines respectent la loi, traitent d'informations liées au monde du hacking au sens premier, celui qui est synonyme d'innovation, de créativité et de liberté. Depuis les débuts de l'ère informatique, les hackers sont en première ligne pour faire avancer notre réflexion, nos standards et nos usages quotidiens.

Mais cela n'a pas empêché notre administration de référence, la «Commission paritaire des publications et agences de presse» (CPPAP) de refuser nos demandes d'inscription sur ses registres. En bref, l'administration considère que ce que nous écrivons n'intéresse personne et ne traite pas de sujets méritant débat et pédagogie auprès du grand public. Entre autres conséquences pour la vie de nos magazines : pas d'abonnements possibles, car nous ne pouvons pas bénéficier des tarifs presse de la Poste. Sans ce tarif spécial, nous serions obligés de faire payer les abonnés plus cher ! Le monde à l'envers...

La seule solution que nous avons trouvée est de proposer à nos lecteurs de s'abonner à une mailing-list pour les prévenir de la sortie de nos publications. Il s'agit juste d'un e-mail envoyé à tous ceux intéressés par nos magazines et qui ne veulent le rater sous aucun prétexte.

Pour en profiter, il suffit de s'abonner directement sur ce site
http://eepurl.com/FlOOD
(le L de «FlOOD» est en minuscule)
ou de scanner ce QR Code avec votre smartphone...



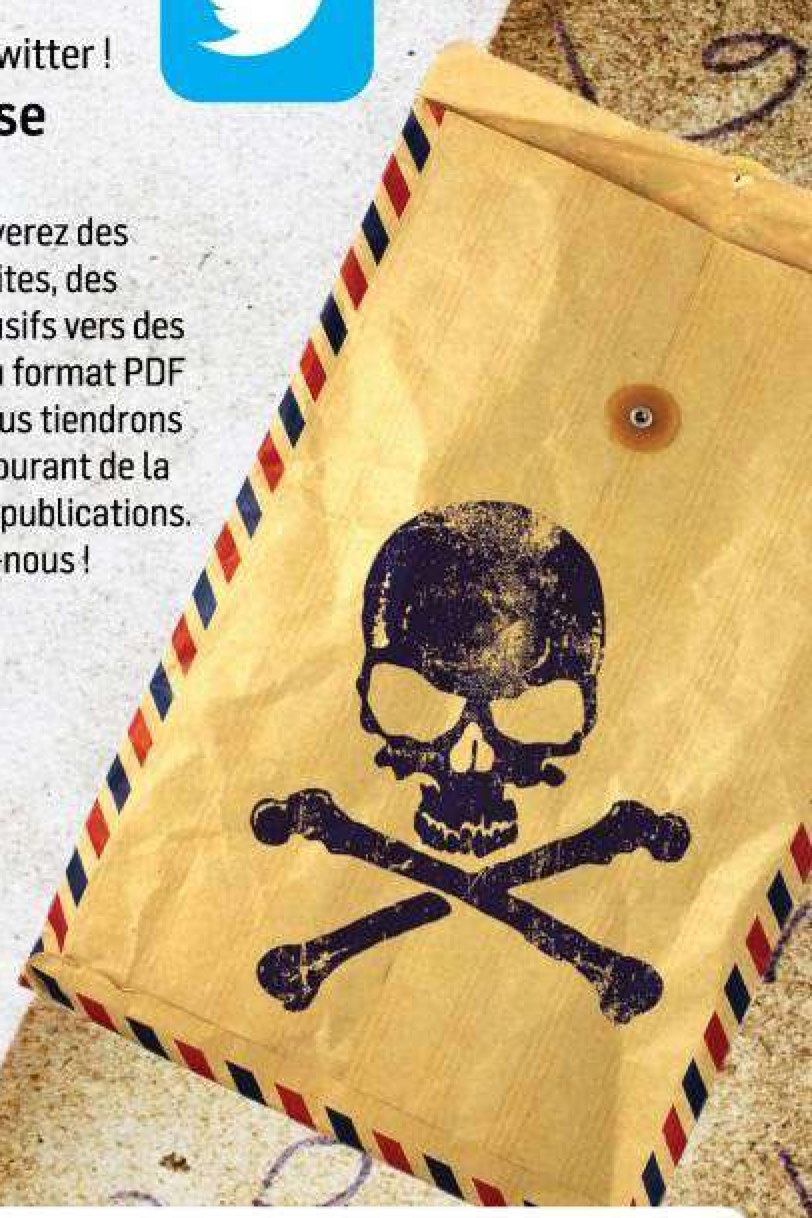
NOUVEAU !

La rédaction se dote d'un compte Twitter !
twitter.com/ben_IDPresse





Vous trouverez des news inédites, des liens exclusifs vers des articles au format PDF et nous vous tiendrons aussi au courant de la sortie des publications. Rejoignez-nous !



TROIS BONNES RAISONS DE S'INSCRIRE :

1 Soyez averti de la sortie de *Pirate Informatique* et des *Dossiers du Pirate* en kiosques. Ne ratez plus un numéro !

2 Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.

3 Votre adresse e-mail reste confidentielle et vous pouvez vous désabonner très facilement. Notre crédibilité est en jeu.

Votre marchand de journaux n'a pas *Pirate Informatique* ou *Les Dossiers du Pirate* ?

Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire. Pour cela, munissez-vous du numéro de codification L12730 pour *Pirate Informatique* ou L14376 pour *Les Dossiers du Pirate*.

Conformément à la loi «informatique et libertés» du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.

TOUT POUR SAUVEGARDER VOTRE SYSTÈME

Avec la quantité de données et de souvenirs présente sur nos ordinateurs et nos smartphones, il faut aimer le goût du risque pour ne pas sauvegarder ses fichiers. Si vous avec une partition de libre, une clé USB ou un disque dur de grande capacité, pourquoi ne pas automatiser cette tâche ?



Même si Microsoft a fait des progrès depuis Vista, le module de sauvegarde de Windows manque encore un peu d'options et d'ergonomie pour les utilisateurs pointilleux que nous sommes : pas de chiffrement et pas de clonage de disque au programme. Si l'on compte aussi l'impossibilité d'accéder aux détails des fichiers, le module de Microsoft est un peu à la traîne. Ici, nous parlons de sauvegardes sécurisées, chiffrées, et paramétrables (tout le système, certains dossiers, quelques fichiers...). N'occultons pas complètement l'outil Windows, qui reste une solution simple et efficace, mais sachez que les outils présentés dans les pages suivantes sont beaucoup plus puissants, pour peu que vous acceptiez de changer un peu vos habitudes.

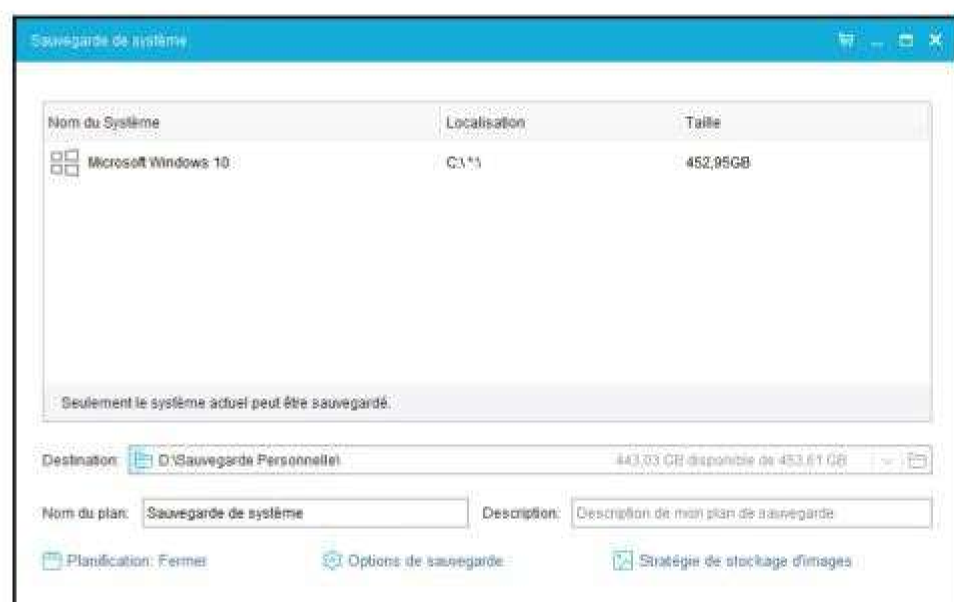
EASEUS TODO BACKUP → LA RÉFÉRENCE

Même dans sa version Free, EaseUS Todo Backup est complet : sauvegarde d'un disque ou d'une partition, d'un groupe de dossiers, du système, planification, sauvegarde sur le réseau, sur un NAS ou un cloud (Google Drive, OneDrive ou Dropbox) et clonage complet de vos disques. Le logiciel permet aussi de créer un disque bootable pour restaurer les données préalablement sauvegardées. Si vous désirez stocker sur des CD ou des DVD, Todo Backup va fractionner votre sauvegarde en paquets de 650 Mo, 700 Mo ou 4,7 Go. Mais ce n'est pas tout. Todo Backup peut aussi effacer de manière sécurisée une partition, créer un disque d'urgence en cas de crash (Linux ou WinPE) et vérifier l'intégrité des différentes images de disque que vous aurez créées.

Lien : **goo.gl/7VvNFt**

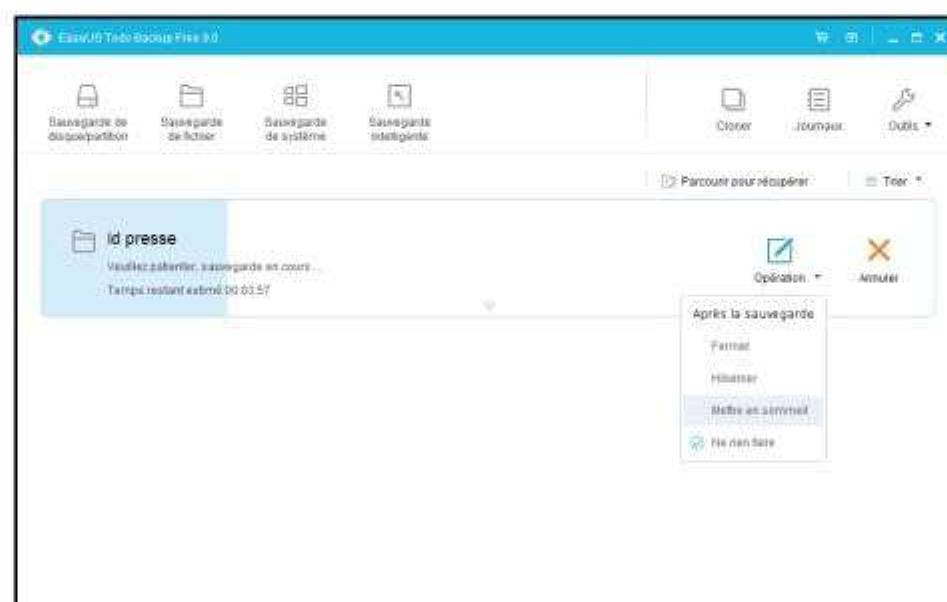
INFOS [EASEUS TODO BACKUP] TUTO

Où le trouver ? [goo.gl/7VvNFt] Difficulté : ☠☠☠



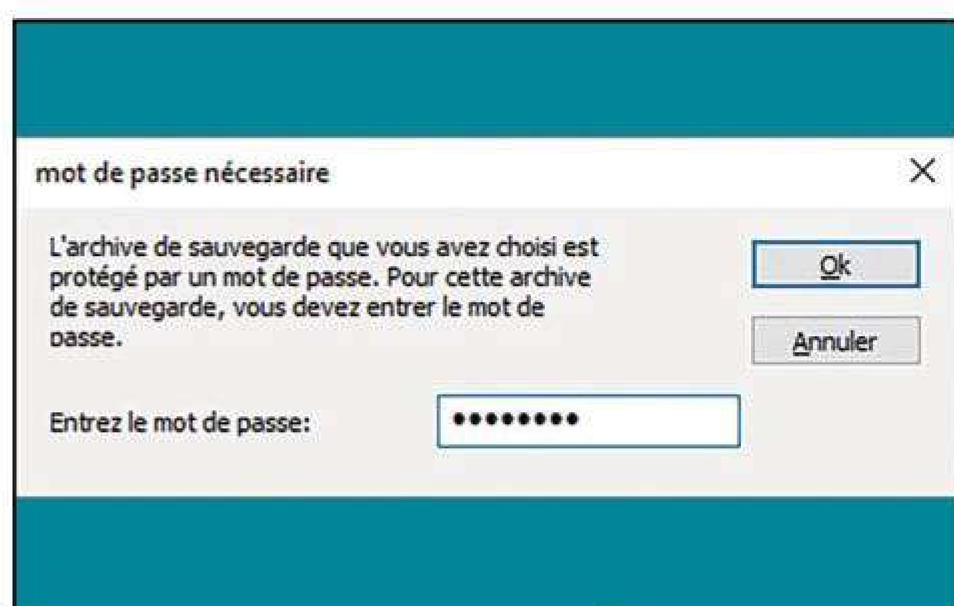
01 › LES TYPES DE SAUVEGARDE

Sauvegarder un disque entier, un fichier ou un dossier précis, ou encore tout le système, EaseUS Todo Backup donne l'embarras du choix. La Sauvegarde intelligente laisse le choix au logiciel de sauvegarder ce qu'il estime essentiel. Chaque fonctionnalité propose un planificateur et des options spécifiques (emplacement, compression, chiffrement et priorité du processus).



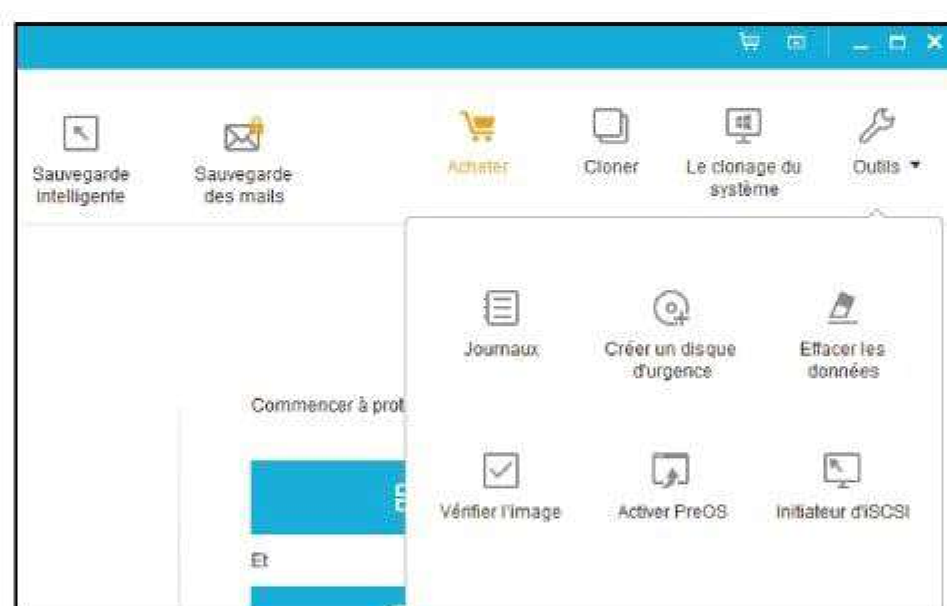
02 › SAUVEGARDER

Après avoir tout paramétré, il suffit de cliquer sur **Procéder**. Durant la sauvegarde, il est possible de demander au logiciel de réaliser une tâche lorsque le processus sera terminé : hiberner, fermer ou mise en veille. C'est sur cette même fenêtre que l'icône de restauration apparaîtra lorsque la sauvegarde sera terminée.



03 › EXPLORER UN FICHIER .PBD

Si vous avez chiffré votre sauvegarde, vous pourrez tout de même explorer son contenu depuis l'explorateur de fichiers Windows, à condition d'avoir installé Todo Backup et d'entrer le mot de passe lorsque vous ouvrez le fichier **.pbd**.



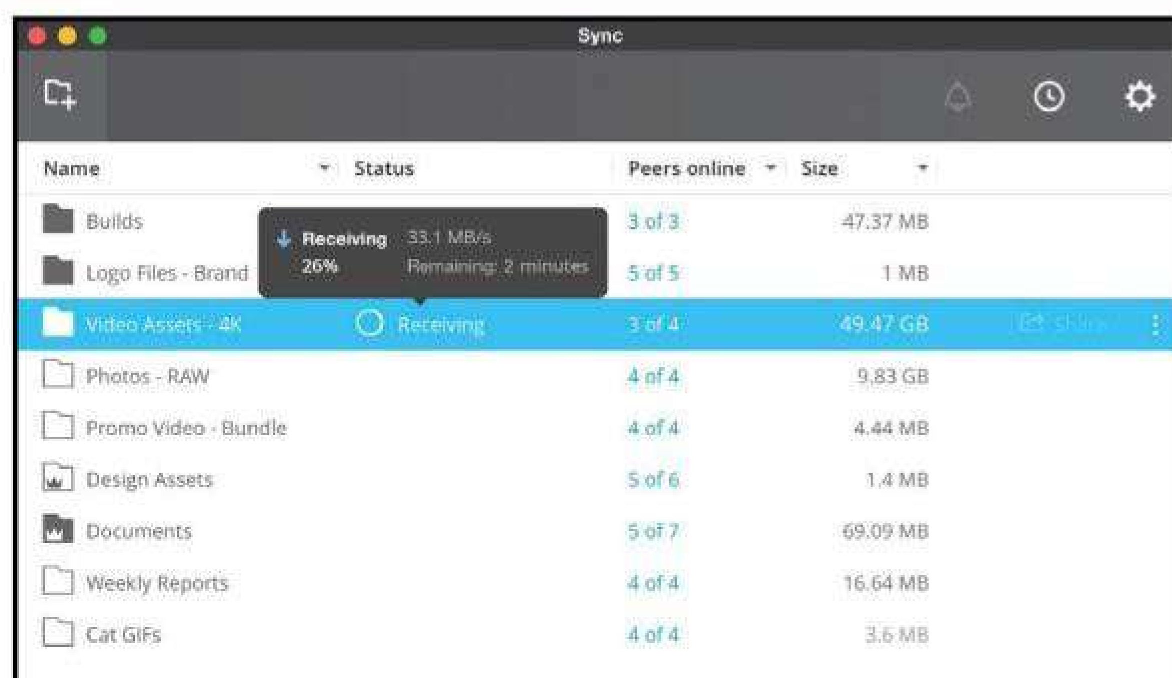
04 › LES AUTRES OUTILS

EaseUS Todo Backup est très complet, même dans sa version gratuite. En cliquant sur **Outils**, vous accédez à plusieurs fonctions intéressantes qui vous épargneront l'installation d'autres logiciels : vérification des images disque, effacement sécurisé, création d'un disque d'urgence, etc. Difficile de ne pas trouver ce que l'on cherche !



Resilio Sync Home → Partage et synchronisation

Celui qui s'appelait encore BitTorrent Sync il y a quelques mois a trois casquettes : il permet de sauvegarder, de synchroniser vos données et de partager du contenu avec vos amis. Comme le système est décentralisé (vos fichiers ne sont pas sur un serveur), la seule limite est celle de la taille de votre disque dur. Grâce à la technologie P2P de BitTorrent, vous synchronisez un ou plusieurs dossiers avec vos amis en leur communiquant une clé secrète unique.



Vos amis n'auront qu'à installer le programme et taper votre clé.C'est aussi un très bon moyen pour avoir accès à tous vos fichiers depuis tous vos appareils (Windows, MacOS, iOS, Android, Windows mobile, Kindle Fire, FreeBSD ainsi que les NAS Netgear). Il faudra juste que votre ordinateur soit allumé pour que vos contacts aient accès aux dossiers.

Difficulté : ☠☠☠

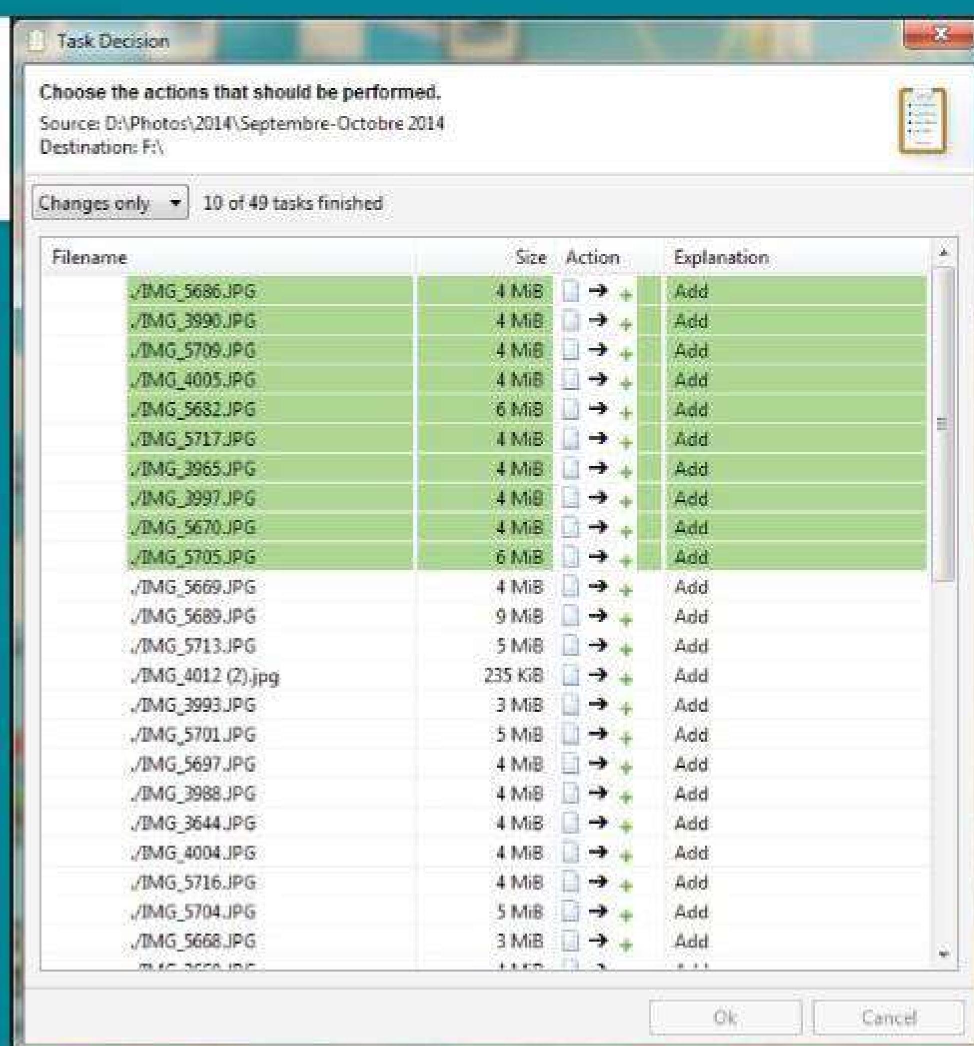
Lien : **www.resilio.com/individuals**

FulSync → Sauvegarde et synchronisation

FullSync est aussi à l'aise avec des sauvegardes simples, incrémentielles ou avec de la synchronisation de fichiers (dans un ou deux sens). Le logiciel autorise aussi l'automatisation des sauvegardes depuis et vers des répertoires locaux, du FTP, du SFTP ou des partages Windows (SMB). Le mode Publish/Update vous permettra même de mettre à jour un site Web à partir d'une copie locale. Bien sûr, tout est paramétrable dans le temps (un oubli est si vite arrivé) et vous disposerez aussi de filtre pour exclure certains fichiers.

Difficulté : ☠☠☠

Lien : **http://fullsync.sourceforge.net**

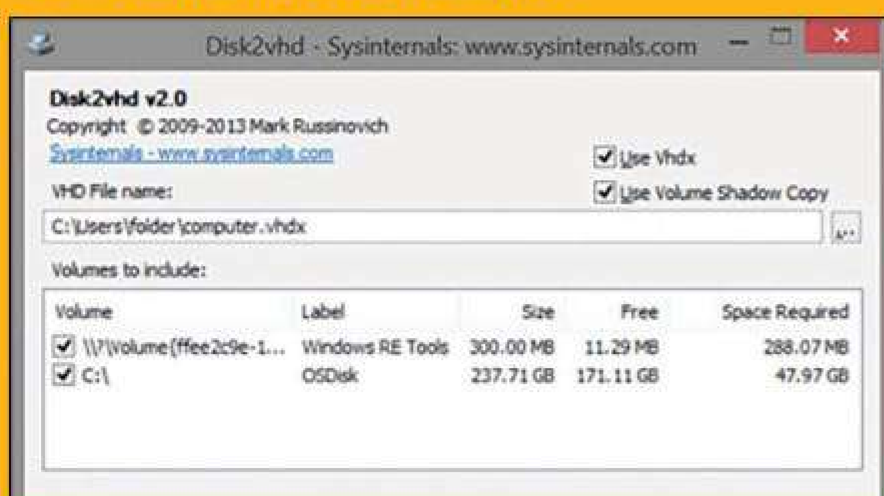


Disk2vhd → Disque dur virtuel

Disk2vhd va créer une image virtuelle d'un disque dur physique. L'image est lue par n'importe quelle machine virtuelle (via Microsoft Virtual PC par exemple, ou d'autres logiciels du genre). L'intérêt est que la sauvegarde peut se faire même pendant l'utilisation du disque (Shadow Copy). Seul l'espace occupé est copié : si votre disque dur de 500 Go contient 5 Go de données, le backup fera 5 Go. Disk2vhd est très simple d'utilisation, ce qui ne gâche rien.

Difficulté : ☠☠☠

Lien : **https://goo.gl/J2ajnN**



CrashPlan → Pour les données

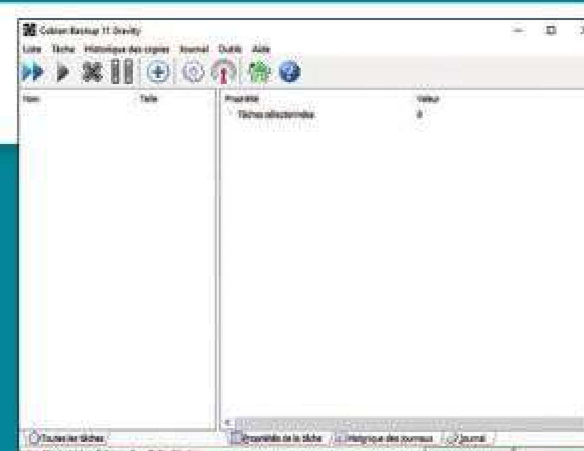
Réservé à la sauvegarde de vos données (fichiers, photos...), CrashPlan, dans sa version gratuite, s'occupe de mettre tout ça sur un périphérique externe, ou sur un autre PC, même si ce dernier n'est pas connecté au même réseau. Les données sont chiffrées avant transmission, qui est elle-même chiffrée. Les sauvegardes incrémentielles et différentielles sont supportées, mais vous ne pouvez programmer qu'une sauvegarde par jour.

Difficulté : ☠☠☠

Lien : **crashplan.com**



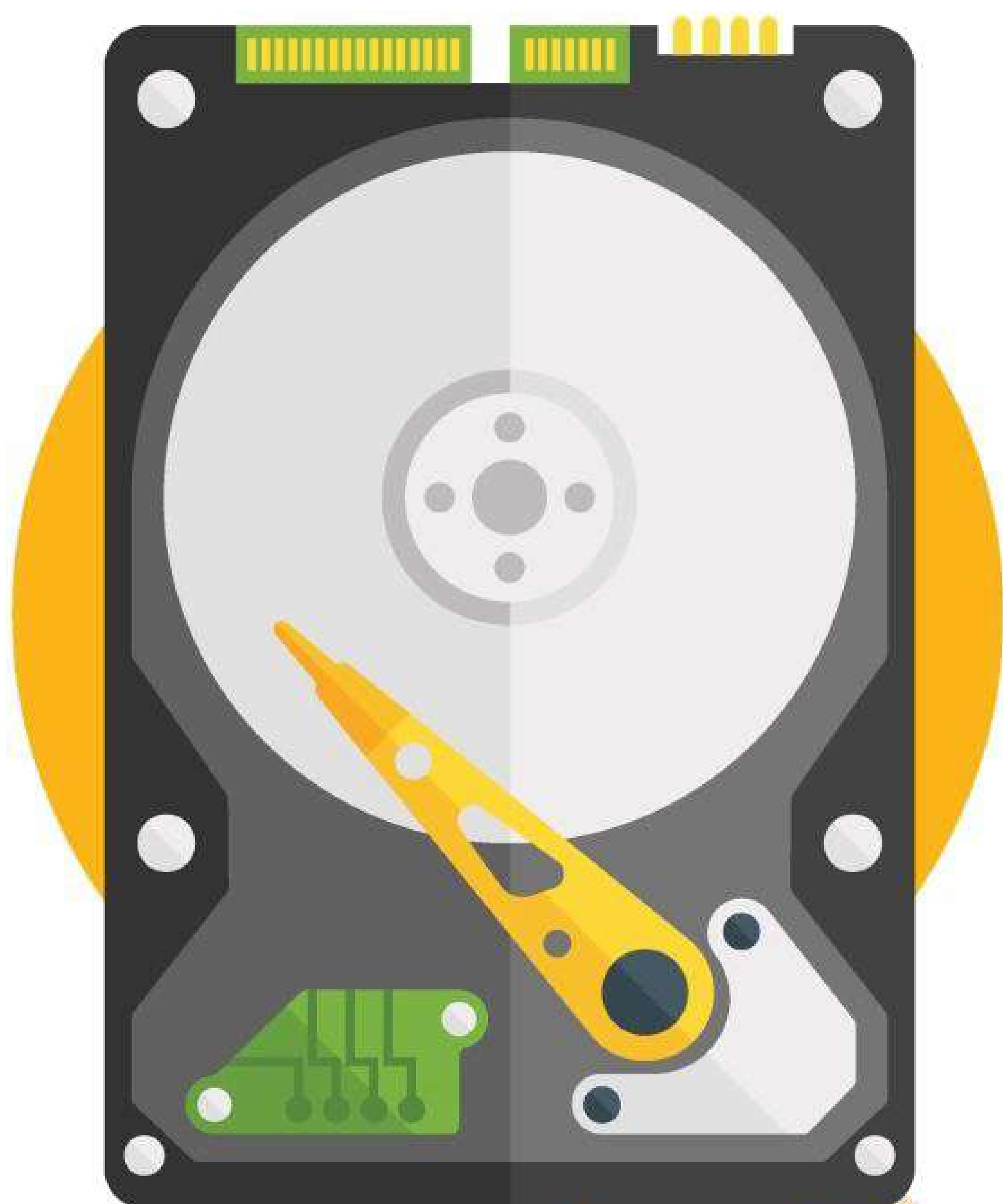
Cobian Backup → Le challenger



Cobian Backup est un autre poids lourd de la sauvegarde. Gratuit et régulièrement mis à jour, il permet presque autant de choses que Todo : sauvegardes standards ou incrémentielles, compression, planification, transfert vers FTP ou un volume disponible sur votre réseau local. Il lui manque cependant le clonage de disque et toutes les petites choses qui font de Todo un cador (disque d'urgence, fractionnement, effacement et sauvegarde du système). Du côté des points forts, on compte un chiffrement AES « complet » et une compatibilité avec la technologie Shadow Copy de Microsoft (création de sauvegardes même si le volume est en activité).

Difficulté : ☠☠☠ Lien : **cobiansoft.com**

UNE IMAGE MIROIR DE VOTRE DISQUE DUR







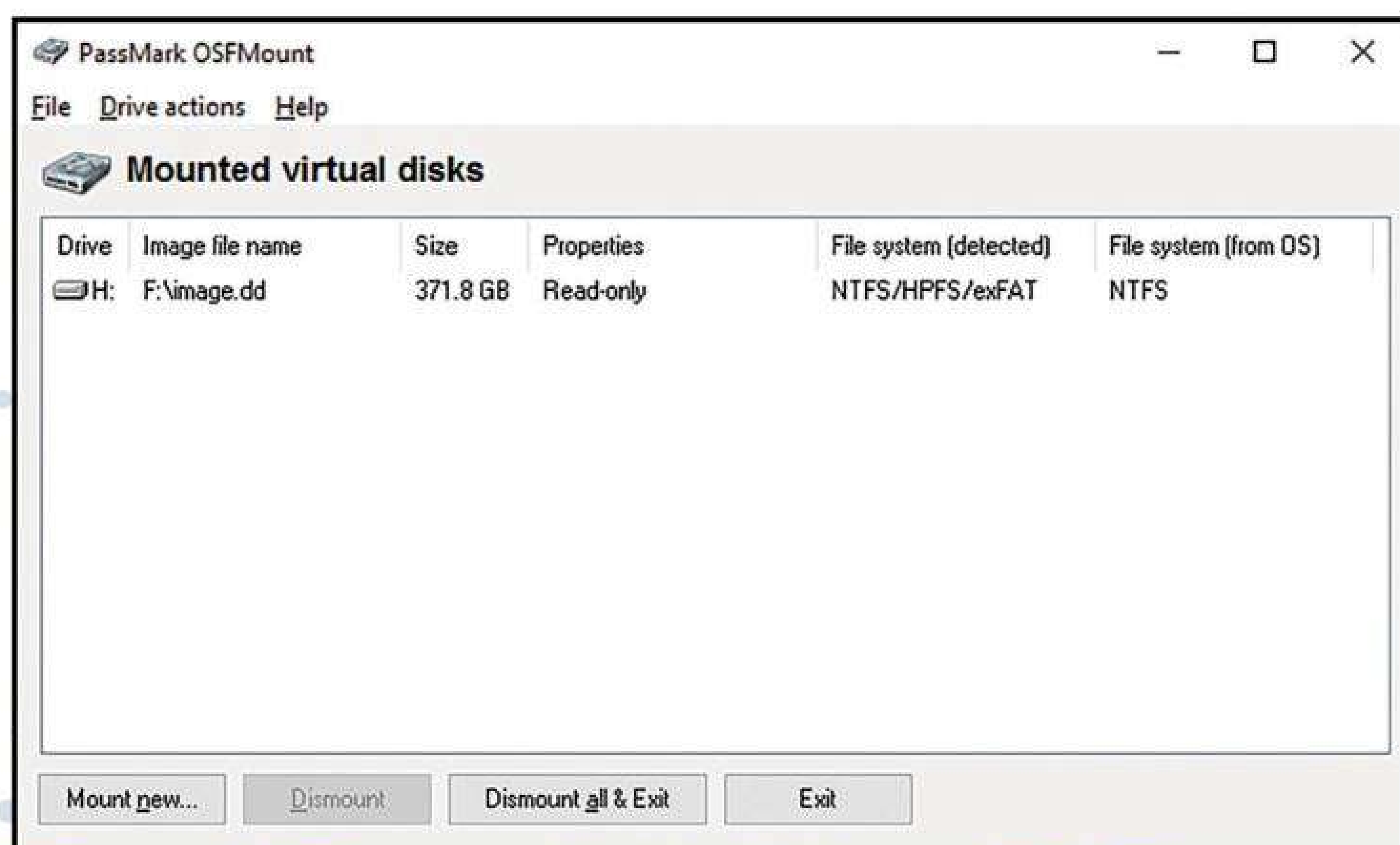
UNE IMAGE IDENTIQUE DE VOTRE DISQUE DUR PERMET DE GAGNER DU TEMPS EN CAS DE PÉPIN MATÉRIEL...

Disponible sous DOS, Windows, Linux et MacOS, TestDisk est un logiciel qui va vous aider à réparer ou récupérer le maximum de données issues d'un disque dur connaissant des problèmes. Le sujet est assez vaste, les cas de figure assez nombreux mais nous avons donc décidé de faire une démonstration inédite avec un scénario catastrophe...

TestDisk est un logiciel français de récupération de données. Il permet de restaurer des partitions perdues et de réparer la table des partitions si celle-ci a été endommagée par un virus ou une erreur de manipulation. Gratuit et open source, TestDisk permet aussi de reconstruire le secteur de boot d'un système de fichiers FAT ou NTFS, de récupérer des fichiers sur presque tous types de partitions (FAT, NTFS ou ext) et de copier les fichiers depuis une partition FAT, NTFS, ext2/ext3/ext4 même si elle est effacée.

NOTRE SCÉNARIO CATASTROPHE

Mais pour notre démonstration, nous allons imaginer un scénario catastrophe : un de vos disques durs fait de drôles de bruits ou a été contaminé par un malware. Plus le temps avance et moins vous avez d'espoir de récupérer vos données. Le mieux est alors de brancher un disque dur de récupération contenant TestDisk et de faire une image de votre disque avant que ce dernier ne lâche complètement. Si votre disque dur contient votre OS, il faudra le démonter pour tenter la récupération sur un autre PC. Il ne faudra surtout rien faire sur le disque en panne sous peine d'écraser des données ou d'accélérer la déliquescence de votre matos. Bien sûr TestDisk fonctionnera avec une clé USB, une carte SD, un CD/ DVD ou un disque dur externe. Une fois l'image créée, nous verrons comment accéder aux fichiers et les restaurer. Notez enfin que TestDisk est contenu dans les CD de réparation dont nous vous parlons souvent : Ultimate Boot CD et Hiren's Boot CD.



Sous Windows, votre fichier image.dd pourra être monté avec le logiciel OSFMount. Votre partition sauvegardée disposera alors de sa propre lettre de lecteur et vous pourrez naviguer à la recherche de vos fichiers perdus.



INFOS [TESTDISK]

Où le trouver ? [**www.cgsecurity.org**] Difficulté :

TUTO

```
C:\Users\benbailleul\Desktop\testdisk-7.0\testdisk_win.exe
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

  TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
 Disk \\.\PhysicalDrive0 - 1000 GB / 931 GiB
 Disk \\.\PhysicalDrive1 - 1000 GB / 931 GiB
>Drive C: - 399 GB / 371 GiB
 Drive D: - 600 GB / 558 GiB
 Drive F: - 500 GB / 465 GiB
 Drive G: - 500 GB / 465 GiB

>[Proceed ]  [  Quit  ]

Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
```

01 › PRÉPARATION

TestDisk ne nécessite pas d'installation, dézippez l'archive et placez le dossier dans le disque dur ou la clé USB qui va servir à accueillir les données. N'oubliez pas que si votre disque dur ou partition à récupérer fait 380 Go, l'image fera 380 Go même s'il ne contient que 152 Go de données. Lancez **testdisk_win.exe** et faites **Create** puis choisissez la partition à sauvegarder. Pour nous ce sera **C:/**.

```
C:\Users\benbailleul\Desktop\testdisk-7.0\testdisk_win.exe
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Drive C: - 399 GB / 371 GiB

Please select the partition table type, press Enter when done.
>[Intel  ] Intel/PC partition
 [EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
 [Humax  ] Humax partition table
 [Mac    ] Apple partition map
 [None   ] Non partitioned media
 [Sun    ] Sun Solaris partition
 [XBox   ] XBox partition
 [Return ] Return to disk selection

Hint: None partition table type has been detected.
Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a disk to be 'Non-partitioned'.
```

02 › LE TYPE DE PARTITION

La suite concerne le choix du type de partition. Normalement TestDisk le détecte automatiquement, mais il peut y avoir des ratés. Si vous avez installé vous-même Windows ou Linux, ou si votre disque est un disque externe (carte SD, clé USB, etc.), il faudra choisir **Intel**. Si vous avez un PC avec un Windows OEM (préinstallé) il faudra choisir **EFI GPT**. Si vous voyez mal vos partitions ou si vous constatez des incohérences, rien ne vous empêche d'essayer une autre option. Il existe des fonctionnalités pour les partitions Mac, Xbox ou Sun Solaris.

```
C:\Users\benbailleul\Desktop\testdisk-7.0\testdisk_win.exe
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Drive C: - 399 GB / 371 GiB
     CHS 48541 255 63 - sector size=512

 [ Analyse  ] Analyse current partition structure and search for lost partitions
>[ Advanced ] Filesystem Utils
 [ Geometry ] Change disk geometry
 [ Options  ] Modify options
 [ MBR Code ] Write TestDisk MBR code to first sector
 [ Delete   ] Delete all data in the partition table
 [ Quit     ] Return to disk selection
```

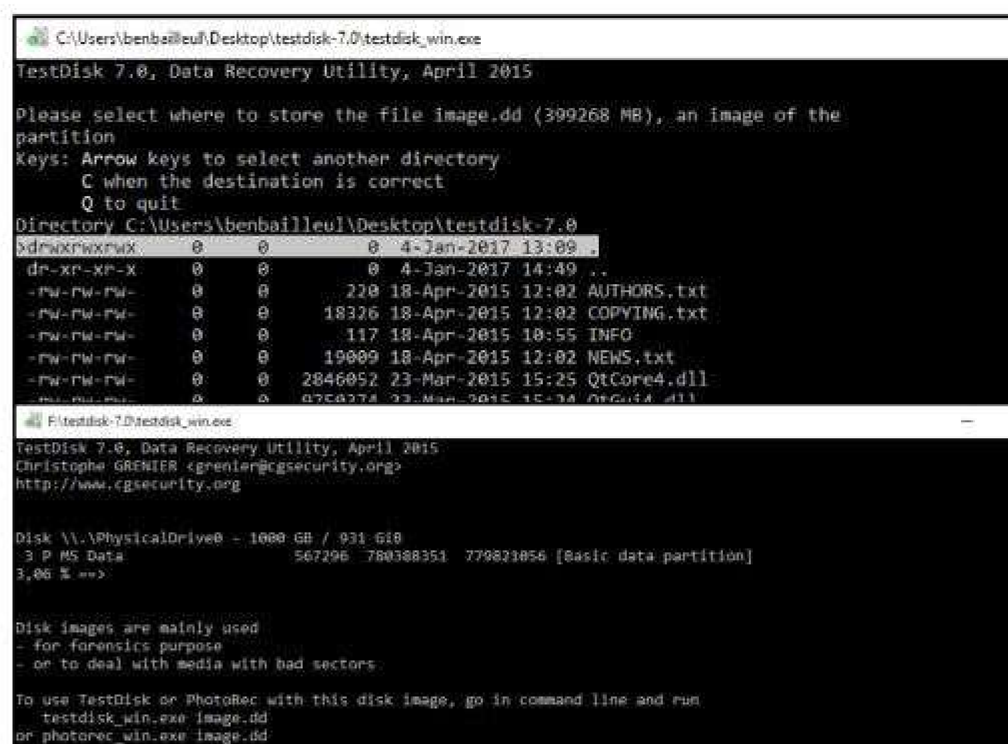
```
C:\Users\benbailleul\Desktop\testdisk-7.0\testdisk_win.exe
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 1000 GB / 931 GiB - CHS 121601 255 63

     Partition                  Start        End    Size in sectors
  1 P EFI System                 2048     534527     532480 [EFI system partition]
  2 P MS Reserved              534528     567295      32768 [Microsoft reserved partition]
> 3 P MS Data                  567296  780388351  779821056 [Basic data partition]
  4 P Unknown               780388352  781410303    1021952 [Basic data partition]
  5 P MS Data               781410304 1953523711 1172113408 [Basic data partition]
```

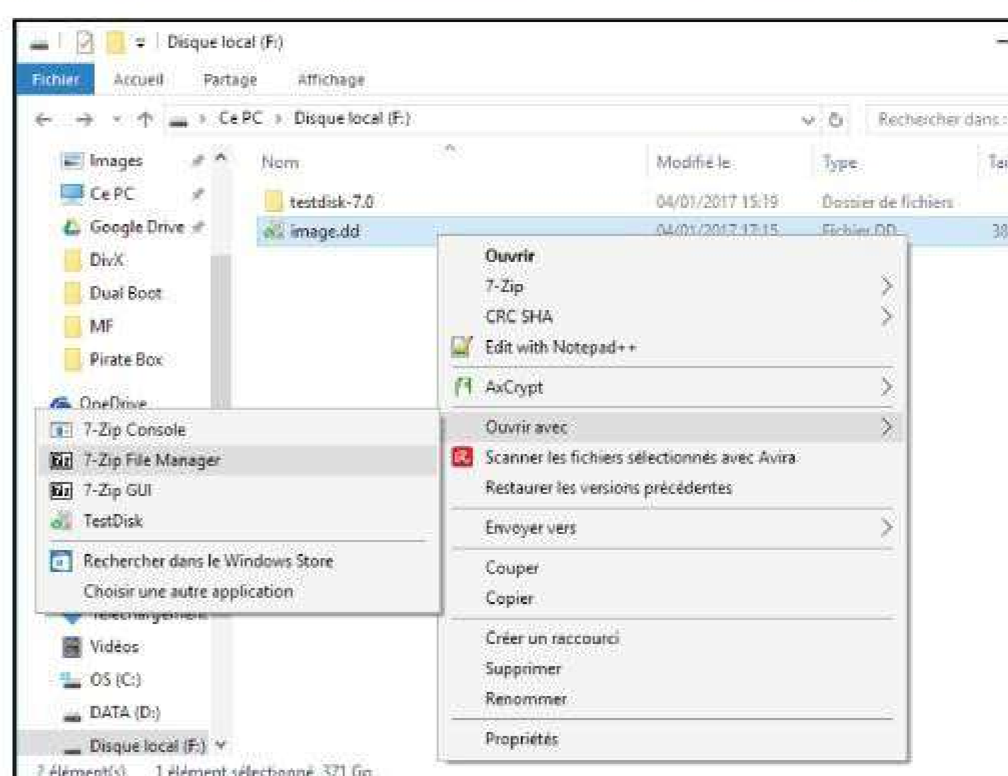
03 › LES ÉLÉMENTS À SAUVEGARDER

Si vous souhaitez récupérer des partitions effacées il faudra choisir **Analyse,** mais pour ce cas de figure, tout est expliqué dans le tuto officiel ici : **https://goo.gl/2rbWQO**. Pour ce que nous voulons faire, il faudra choisir **Advanced**. Retrouvez votre partition en vous aidant de la taille et de l'ordre. Tout ce qui est **EFI System**, **Unknown** ou **Reserved** sont des partitions de sauvegarde, de boot ou de swap.



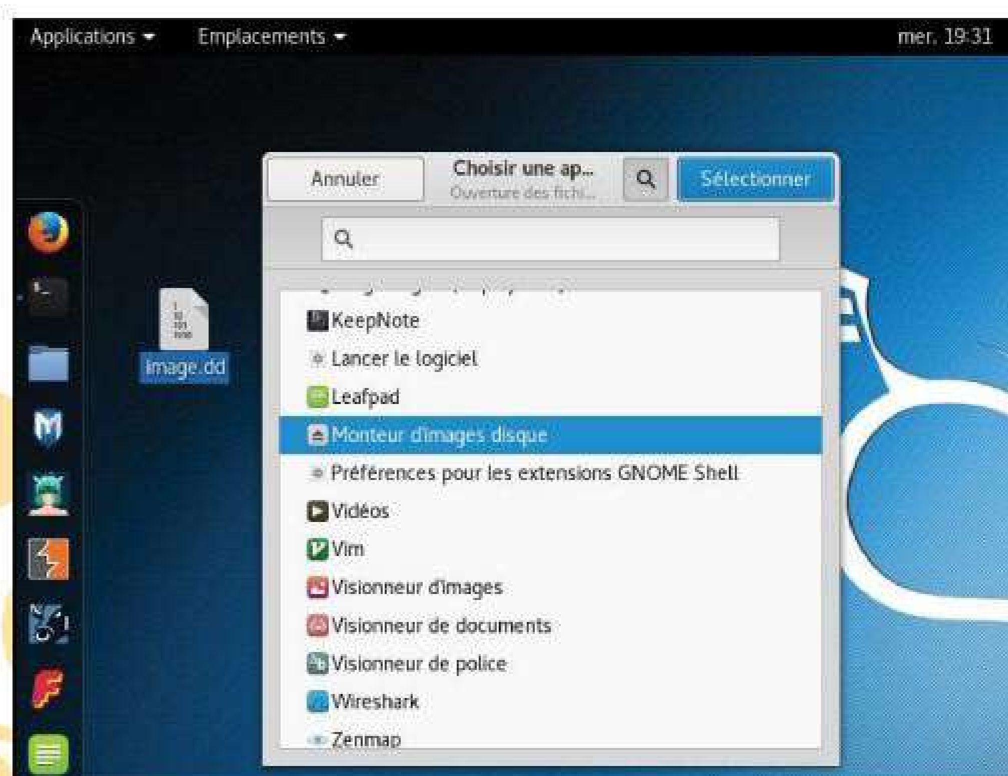
04 › L'EMPLACEMENT DE LA SAUVEGARDE

Il faudra ensuite choisir l'endroit où vous allez stocker cette image de disque. Baladez-vous dans l'arborescence du disque de sauvegarde (vous n'aurez pas accès aux autres disques) et faites **C** lorsque tout est OK. L'image va être copiée. Si le logiciel plante, il reprendra où il en était. Le processus a pris presque 1 heure et demie pour un disque dur de 380 Go. Bravo, votre **image.dd** est sur votre disque de sauvegarde.



05 › ACCÉDEZ AUX FICHIERS

Mais que faire avec ce fichier ? Et bien sous Windows vous pouvez la monter comme une image de jeu avec le logiciel OSFMount par exemple. Mais vous pouvez aussi l'ouvrir avec le File Manager de 7-Zip que vous avez sûrement déjà sur votre PC. Il suffira de faire un clic droit puis **Ouvrir avec...** et de trouver le logiciel **7-ZipFM** dans votre disque dur. Le fichier **.dd** s'ouvrira alors comme une archive et vous pourrez récupérer les fichiers que vous souhaitiez sauver d'une mort certaine ! Vous pouvez aussi ouvrir ce fichier **.dd** avec PhotoRec (voir notre encadré).



06 › ET SOUS LINUX ?

Sous Linux le programme fonctionne de la même manière. Il est disponible de base sous Kali (tapez juste **testdisk** après le prompt), mais si vous avez une autre distribution, il faudra l'installer et le lancer avec **sudo ./testdisk**. Si votre PC ne contient qu'un Linux, le choix du type de partition sera **Intel**. Lorsque votre **image.dd** sera sauvegardée, il faudra la monter avec le **Monteur d'images disque**. Sous Kali, faites un clic droit, **Ouvrir avec une autre application** puis **Afficher toutes les applications** et enfin **Monteur d'images disque**. Votre image sera accessible dans le même dossier et vous pourrez accéder au contenu.

RÉCUPÉREZ PHOTOS ET FICHIERS PERDUS !

Que vous soyez maladroit ou malchanceux, il vous est forcément déjà arrivé d'effacer par inadvertance un ou plusieurs fichiers indispensables : photo, vidéo, MP3, PDF, etc. Le logiciel que nous vous proposons va sans doute vous tirer une sacrée épine du pied...



PhotoRec est, comme son nom l'indique, un logiciel de récupération de photos, mais aussi de tout fichier multimédia, de bureautique ou archive. Quelque soit le support, PhotoRec se chargera d'éviter les drames liés à la perte de vos données : SD, CompactFlash, Memory Stick, Secure Digital, MMC, disque dur, clé USB, CD, DVD, etc. Il fonctionne de la même manière que Recuva. Quand un fichier est supprimé, les métadonnées sont supprimées du système de fichier : nom de fichier, date/heure, taille, etc. Mais les données sont toujours présentes sur le support jusqu'au moment où celles-ci seront écrasées par de nouvelles données. PhotoRec ne nécessite pas d'installation. Il n'ira donc jamais écrire sur votre disque dur ou autre support mémoire que vous voulez récupérer. Vous éviterez donc d'écraser les données que vous essayez de récupérer à tout prix. Mais pour récupérer vos précieux fichiers, PhotoRec va déterminer la taille des blocs puis va les analyser avec une base de signatures. Par exemple le logiciel sait qu'un fichier JPEG va commencer par tels caractères. Que le fichier soit partitionné ou pas, PhotoRec va le retrouver sauf si trop de temps s'est écoulé et qu'il n'arrive pas à récupérer un ensemble d'octets cohérents.

INCLUS AVEC TESTDISK

Sachez que vous pouvez l'utiliser tel quel ou à partir d'une image miroir au format .dd généré par TestDisk. En effet, PhotoRec est fourni avec ce logiciel. Si vous avez perdu des fichiers que vous voulez récupérer, mais que vous êtes obligé de travailler sur cette machine, faîtes un clone de votre disque et traitez-le avec PhotoRec pour éviter de réécrire sur les secteurs où sont stockées vos précieuses données ! Notez enfin que PhotoRec est inclus dans beaucoup de Live CD de récupération comme : Medicat (*voir Pirate Informatique n°33*), Gparted Live CD, System RescueCD ou Ultimate Boot CD.



INFOS [PHOTOREC]

Où le trouver ? [**www.cgsecurity.org/wiki/PhotoRec_FR**] Difficulté : ☠☠☠

TUTO



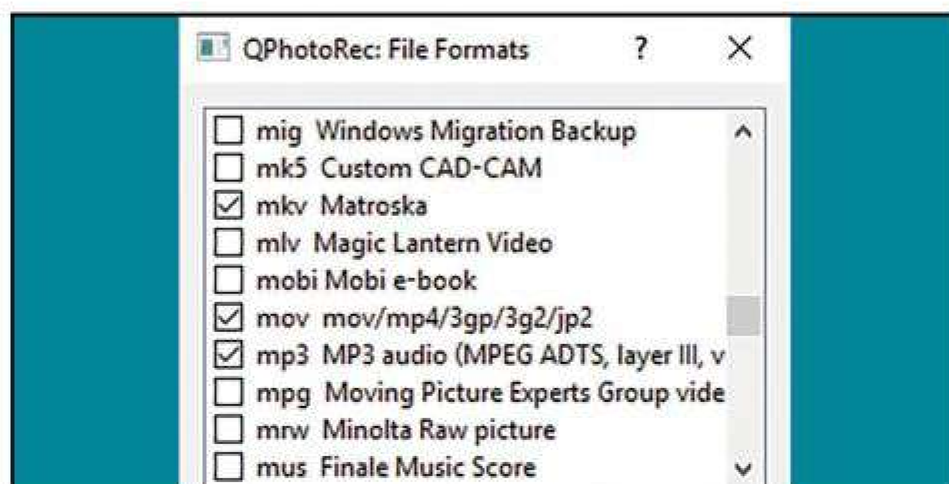
01 › PREMIER CONTACT

PhotoRec est intégré à TestDisk. Vous trouverez ces logiciels pour tous les types d'OS: Windows, Linux, MacOS, FreeBSD, Solaris, etc. PhotoRec dispose toujours d'une version sans interface graphique, mais sous Windows, nous allons tester celle qui dispose d'un GUI: **qphotorec_win.exe**. Pour y accéder, il faudra juste ouvrir l'archive de TestDisk et double-cliquer sur ce fichier EXE. Pour ceux qui utilisent PhotoRec sous un autre OS, il faudra d'abord pointer vers le disque dur, la partition ou le volume où vous avez perdu des fichiers puis spécifier le système de fichier (FAT32, NTFS, ext4, etc.) et pointer vers une destination de sauvegarde (une autre partition, une clé USB, etc.)



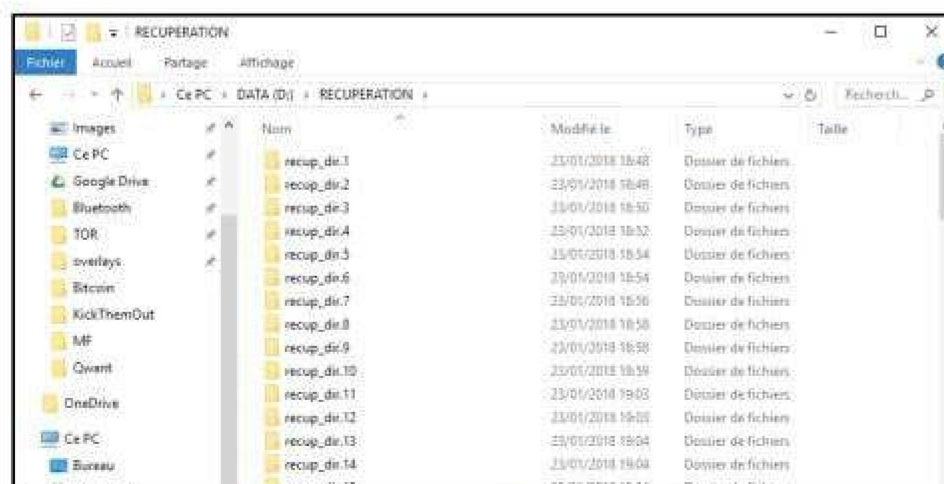
02 › LES RÉGLAGES

Mais revenons à notre version Windows avec son interface graphique. Imaginons un scénario où nous aurions supprimé par erreur des fichiers dans un dossier sur C. Dans le menu déroulant, sélectionnons la partition puis le système de fichier (ici NTFS). Sélectionnons ensuite **Free** pour rechercher dans l'espace «libre» du disque dur (**Whole** recherchera dans l'ensemble du volume, mais ce serait une perte de temps dans notre cas de figure). Sélectionnez ensuite une destination de sauvegarde pour vos fichiers perdus qui ne sera pas localisée sur la même partition. Dans notre exemple ce sera un dossier dans D.



03 › LES TYPES DE FICHIERS

Si vous avez souvenance de ce que vous avez potentiellement perdu, vous pouvez spécifier les fichiers cibles. Pour nous, ce sera des fichiers .7z, .jpeg, .pdf, .png, .torrent, .zip et .doc. Vous gagnerez du temps en faisant le distingo, mais si vous ne vous souvenez plus du détail, vous n'êtes pas obligé de spécifier. Attention , il faudra quand même cibler vos fichiers (multimédia, bureautique, etc.) car sinon la recherche va vous prendre des heures, surtout sur des volumes conséquents.

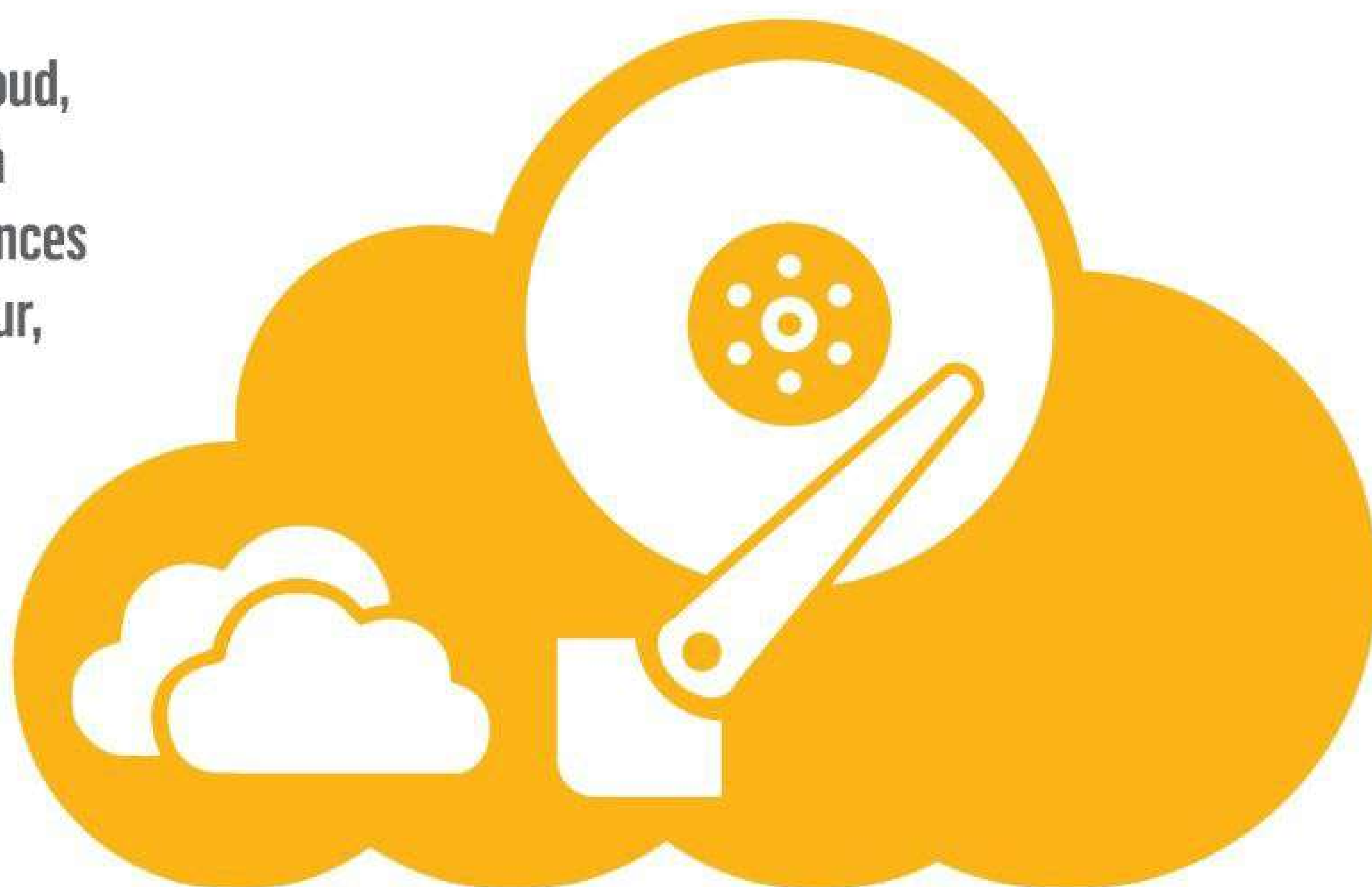


04 › C'EST GAGNÉ!

Lorsque vous aurez atteint 100%, faites **Quit** et dirigez-vous vers le dossier de sauvegarde que vous aurez spécifié. Il y aura plusieurs dossiers. Ces derniers seront classés par ordre chronologique de leur restauration. Si vous spécifiez trop de types de fichiers, vous aurez bien du mal à retrouver les vôtres. Ici nous avons retrouvé nos photos effacées par erreur. Sauvegardez-les bien maintenant!

SAUVEGARDEZ DANS LE CLOUD

Copiés dans le Cloud, vos fichiers sont à l'abri des défaillances de votre ordinateur, ou d'erreurs de manipulation.



Le but premier du stockage dans le Cloud, c'est de vous permettre d'accéder à vos données depuis n'importe où, votre ordinateur bien sûr, mais aussi n'importe quel PC connecté à Internet, et vos appareils mobiles. Avantage collatéral, la copie de vos fichiers sur des serveurs Internet constitue une excellente sauvegarde, que vous n'avez même pas à vous soucier de mettre à jour régulièrement, puisque grâce à la synchronisation tout changement d'un document sur votre ordinateur est automatiquement répercuté sur son double en ligne. N'importe quel service de Cloud fait l'affaire, de préférence avec un logiciel client à télécharger (les accès sont plus simples). Nous utilisons ici celui de Microsoft, OneDrive, qui présente l'avantage d'être préinstallé dans Windows 10. Avec Windows 7, il suffit de souscrire au service, puis de télécharger et installer le logiciel client.

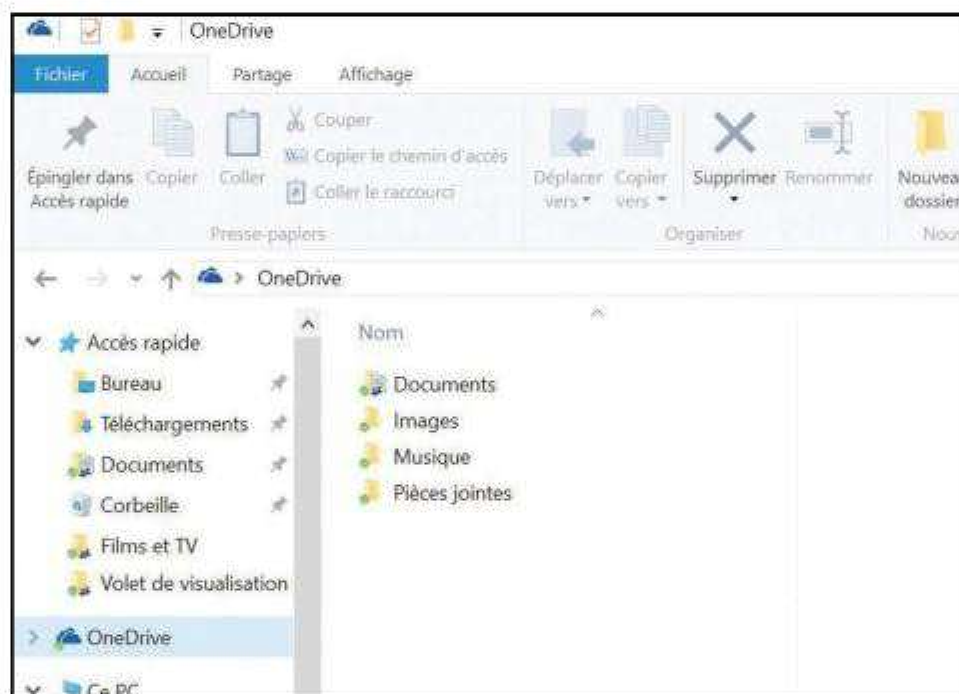


LE CLOUD C'EST PRATIQUE, MAIS N'OUBLIEZ PAS D'AJOUTER VOUS-MÊME UNE COUCHE DE CHIFFREMENT !



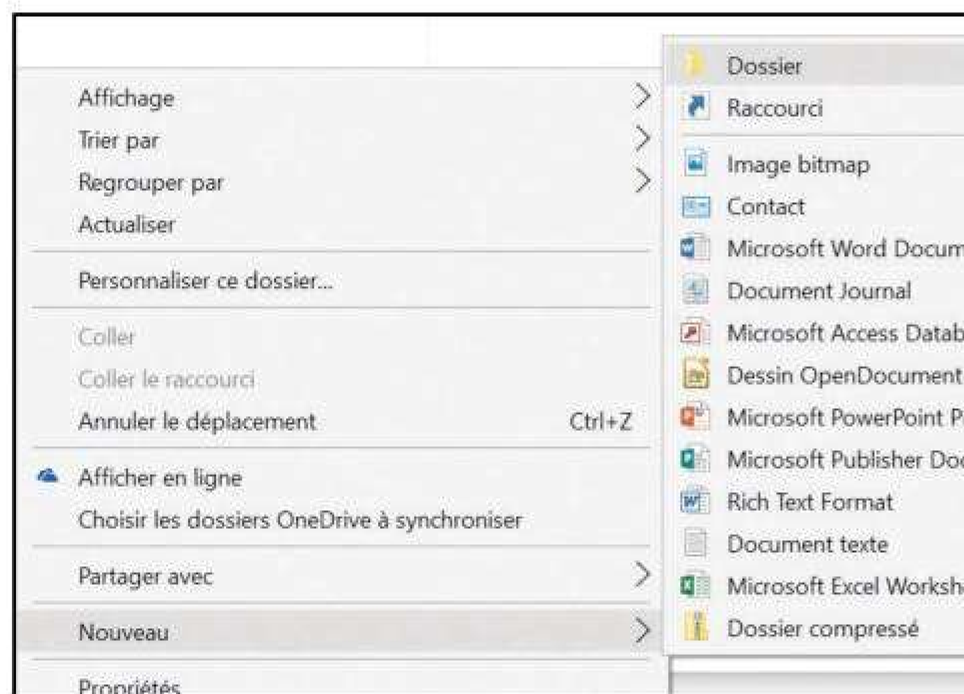
INFOS [ONEDRIVE]
Où le trouver ? [https://onedrive.live.com] Difficulté :

TUTO



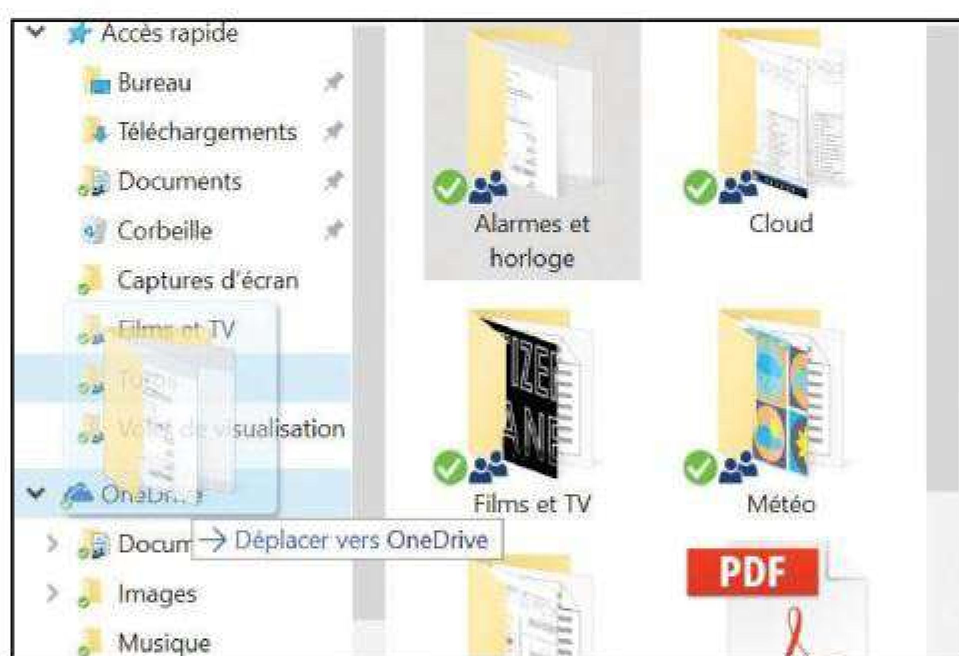
01 › ACCÉDER À ONEDRIVE

Ouvrez l'Explorateur de fichiers et cliquez sur l'icône **OneDrive**, dans le volet de navigation, à gauche. Vous y trouvez une série de dossiers présents par défaut: **Documents, Images, Musique...** C'est l'exact reflet de votre espace en ligne, hébergé sur les serveurs de Microsoft.



02 › ORGANISER LES DOSSIERS

Vous pouvez structurer librement le dossier OneDrive, exactement comme les autres dossiers de votre disque dur: supprimer des dossiers (clic droit dessus, **Supprimer**), les renommer (clic droit **Renommer**), en créer de nouveaux (clic droit, **Nouveau** puis **Dossier**)...



03 COPIER DANS LE CLOUD

Pour copier un fichier ou un dossier dans votre espace en ligne, il suffit de le déplacer dans le dossier OneDrive: faites un clic droit dessus et choisissez **Couper**, puis allez dans le dossier OneDrive de destination, faites un clic droit à l'intérieur et choisissez **Coller**. Vous pouvez aussi utiliser le glisser-déposer.

Synchroniser vos fichiers OneDr
Les fichiers que vous synchronisez occuperont de l'espa
Synchroniser tous les fichiers et dossiers de m
Synchroniser uniquement ces dossiers
Fichiers qui ne sont pas dans un dossier (0,0 Ko)
Documents (16,7 Mo)
Fichiers dans « Documents » (617,4 Ko)
Modèles Office personnalisés (0,0 Ko)
Tutos (16,1 Mo)
Images (767,0 Ko)

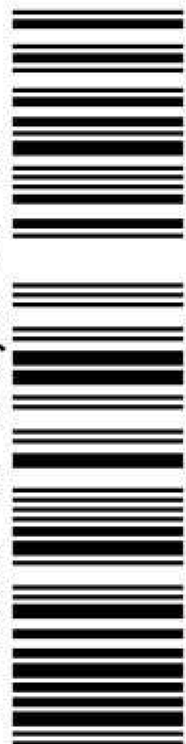
04 › RÉGLER LA SYNCHRONISATION

Faites un clic droit sur l'icône OneDrive, puis **Choisir les dossiers OneDrive à synchroniser**. Décochez les dossiers dont vous ne souhaitez pas avoir une copie sur votre PC. Ils sont effacés du dossier OneDrive (mais restent disponibles en ligne). Pratique pour éviter la copie de vos photos perso sur votre PC au bureau.

UN COUP DE FATIGUE OU UN GROS PROBLÈME ?

Réparez et dopez vous-même votre PC !







BEL/LUX : 4,60 € - DOM : 4,70 € - PORT.CONT. : 4,60 € - GH : 6 FS - CAN : 6,99 $
CAD - MAR : 43 MAD – TUN : 6,4 TND - NCAL/S : 650 CFP - POL/S : 660 CFP